Pages 1 through 16 redacted for the following reasons:
- -
(b)(5) - Draft
Records under the cognizance of U.S. Central Command

From: Armistead Maj Michael W
To: Rogers Col Daniel S; (b)(6) Masur Col Daniel R; (b)(6)
Cc: (b)(6)
Subject: FW: Wikileaks video (UNCLASSIFIED)
Date: Friday, April 16, 2010 5:10:46 PM
Attachments: CENTCOM Pressrel Farah video APR 2010 (2).doc
USCENTCOM Farah Investigation PAG (24 Jun 09).doc
PROPOSED PUBLIC AFFAIRS GUIDANCE FOR INCIDENTS IN AFGHANISTAN (ver 5 SOCOM edits).docx

---

Gentlemen,

SOCOM Public affairs informed me today that the B1 bomber video from a the battle at Bala Baluk, Farah province in May of 2009 may be leaked through wikileaks within the week, perhaps as early as Monday. If you recall, this is the incident in which our units were accused of killing 140 civilians in an airstrike. It also prompted several articles exclaiming "Rumsfeld's Renegade unit blamed for Afghan deaths. Below and attached is the feedback I received from CFSOCC-A.
CENTCOM will have lead on all responses. I have also attached the PAG we drafted and sent forward after the incident.
I will keep you posted on any further guidance that I receive on this matter.

Note: Wikileaks also posted the video showing reuters journalists with insurgents being killed by AH 64s, FOIA'd by Reuters.
http://wikileaks.org/

r/Maj Armistead

Michael Warren Armistead
Major, USMC
MARSOC Public Affairs
(b)(6)

-----Original Message-----
From: Nye, Edward T COL MIL USA CFSOCC-A PAO (b)(6)
Sent: Friday, April 16, 2010 14:23
To: Armistead Maj Michael W
Cc (b)(6)
Subject: RE: Wikileaks video (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: ~~FOUO~~

Classification: UNCLASSIFIED
Caveats: ~~FOUO~~

Mike,

There is some thought that the next possible WikiLeak may be the Farah incident. If it is CENTCOM has the LEAD backed by ISAF/SOCOM. MARSOC should refer all queries to CENTCOM via SOCOM. The incident

took place while deployed so MARSOC should not respond directly to any questions referencing actions on the ground.

I don't know anymore about the incident than what I read in the documents but I don't think the ground force will be the object of the questions.

WikiLeak has posted information that they plan on posting more of these types of gun camera footage in the future. My sense is that all commands will be hot with these leaks at some point but that CENTCOM or ISAF will take the lead on the majority of them.

Nye

COL Tim Nye
CFSOCC-A PAO
(b)(6)

-----Original Message-----
From: Armistead Maj Michael W (b)(6)
Sent: Friday, April 16, 2010 10:40 PM
To: Nye, Edward T COL MIL USA CFSOCC-A PAO
Subject: Wikileaks video

Sir,

During an earlier conversation with (b)(6) informed me about a possible wikileaks video regarding a raid that involved MARSOC and civcas from May of 2009.
Do you have an additional information that might be helpful to give my boss a heads-up?

r/

Michael Warren Armistead
Major, USMC
MARSOC Public Affairs
(b)(6)

Classification: UNCLASSIFIED
Caveats: ~~FOUO~~

Classification: UNCLASSIFIED
Caveats: ~~FOUO~~

From: (b)(6)
To: Armistead Maj Michael W; (b)(6)
Cc: (b)(6)
Subject: "WIKILEAKS" WEBSITE GUIDANCE DO NOT ACCESS
Date: Thursday, September 2, 2010 12:44:59 PM
Importance: High

PAO, Is this something we should post on the Daily OMB?

Semper Fi

(b)(6)

Amateurs Talk Tactics...Professionals Talk Logistics

****

USMC Personnel (Marines/Civilians/Contractors) are hereby cautioned and directed to NOT access the WIKILEAKS website from a personally owned, publically owned or US Government computer system. By willingly accessing the WIKILEAKS website for the purpose of viewing the posted classified material - these actions constitute the unauthorized processing, disclosure, viewing, and downloading of classified information onto an UNAUTHORIZED computer system not approved to store classified information. Meaning they have WILLINGLY committed a SECURITY VIOLATION.

Not only are these actions illegal, but they provide the justification for security managers to immediately remove, suspend "FOR CAUSE" all security clearances and accesses. Commanders may press for Article 15 or 32 charges, and USMC personnel could face a financial hardship as civilian and contractor personnel will be placed on "Administrative Leave" pending the outcome of a NCIS investigation.

Do not ask family or friends to access the website from their home computer.

Please pass this information to ALL HANDS: If they purposely accessed the "WIKILEAKS" website to view classified info - they have willingly placed classified information on an open network not authorized to view classified information and have willingly committed a security violation.

DTG: 021330Z Aug 10Precedence: ROUTINEDAC: General
To: AL 72(UC)
UNCLASSIFIED//
RATUZYUW RUCXSSO9296 2141449-UUUU--RHMFIUU.
ZNR UUUUU
R 021330Z AUG 10
FM SSO NAVY WASHINGTON DC//MSD2//
TO AIG 72
INFO RUCXSSO/SSO NAVY WASHINGTON DC//MSD2// BT UNCLAS QQQQ ALL COMMANDS HOLD AND PASS TO SPECIAL SECURITY OFFICER (SSO'S)
SUBJ: BANIF 020-10, THE "WIKILEAKS" WEBSITE GUIDANCE
REFS: (A) ALCON JAG NEWS OF 29 JULY 2010 1. IAW REFERENCE (A) THE BELOW IS PROVIDED AND "QUOTED".
2. "DON PERSONNEL SHOULD NOT ACCESS THE WIKILEAKS WEBSITE TO VIEW OR DOWNLOAD THE PUBLICIZED CLASSIFIED INFORMATION. DOING SO WOULD INTRODUCE POTENTIALLY CLASSIFIED INFORMATION ON UNCLASSIFIED NETWORKS. THERE HAS BEEN RUMOR THAT THE INFORMATION IS NO LONGER CLASSIFIED SINCE IT RESIDES IN THE PUBLIC DOMAIN. THIS IS NOT TRUE.
EXECUTIVE ORDER 13526, SECTION 1.1(4)(C) STATES "CLASSIFIED INFORMATION SHALL NOT BE

DECLASSIFIED AUTOMATICALLY AS A RESULT OF ANY UNAUTHORIZED DISCLOSURE OF IDENTICAL OR SIMILAR INFORMATION."
THE SUBJECT INFORMATION WAS NEITHER PROPERLY NOR IMPROPERLY "DECLASSIFIED" BY AN APPROPRIATE AUTHORITY AND REQUIRES CONTINUED CLASSIFICATION OR RECLASSIFICATION. IT IS "APPARENTLY CLASSIFIED INFORMATION" THAT APPEARS TO HAVE BEEN DISCLOSED WITHOUT APPROPRIATE REVIEW AND AUTHORITY. THE INFORMATION POSTED NEEDS TO BE REVIEWED BY THE APPROPRIATE ORIGINAL CLASSIFICATION AUTHORITIES (OCAS) TO: DETERMINE IF IT IS CLASSIFIED, CONDUCT DAMAGE ASSESSMENTS, AND MAKE A DETERMINATION REGARDING CONTINUED CLASSIFICATION. DESPITE CIRCUMSTANCES SURROUNDING THE WIKILEAKS, CONTINUE TO PROTECT SIMILAR OR IDENTICAL INFORMATION COMMENSURATE WITH THE LEVEL OF CLASSIFICATION ASSIGNED PER SECNAV M-5510.36, UNTIL THE INFORMATION IS ASSESSED BY THE APPROPRIATE OCAS. PLEASE REMEMBER, GOVERNMENT INFORMATION TECHNOLOGY CAPABILITIES SHOULD BE USED TO ENABLE OUR WAR FIGHTERS, PROMOTE INFORMATION SHARING IN DEFENSE OF OUR HOMELAND, AND TO MAXIMIZE EFFICIENCIES IN OPERATIONS. IT SHOULD NOT BE USED AS A MEANS TO HARM NATIONAL SECURITY THROUGH UNAUTHORIZED DISCLOSURE OF OUR INFORMATION ON PUBLICLY ACCESSIBLE WEBSITES OR CHAT ROOMS."
3. JAG POC IS (b)(6) OJAG/NLSC SECURITY MANAGER, OJAG/CODE 30, NATIONAL SECURITY LITIGATION LAW DIVISION, COMM: (b)(6)
DSN: (b)(6)
4. MINIMIZE CONSIDERED. RELEASED BY SSO NAVY, (b)(6)
SSO NAVY POC IS (b)(6)
(b)(6)
BT
#9296
NNNN

US Marine Corps HQMC Public Affairs Media Branch

03 Dec 10

Briefing Cards: Wikileaks – British "failure" in Helmand

BACKGROUND

Among the diplomatic cables released by Wikileaks are some that cite Afghan and American officials as saying that British forces "failed" in their mission to stabilize Helmand province and defeat the Taliban. Media may associate the decision to replace British troops with Marine units in some areas of operation in Helmand as a consequence of that alleged failure.

Coverage:
http://ebird.osd.mil/ebfiles/e20101203792696.html

KEY POINTS/TALKING POINTS

- We're not going to discuss particular wiki-leaks disclosures, but can tell you that UK forces made great sacrifices and set the conditions for success in Sangin.

- Sangin is a still a tough fight. Because of the success of the 40 Commando, the Marines are able to expand the security pocket out to areas that have never seen the presence of coalition forces. This area is the very bedrock of where the insurgent has been able to hide, refit, retrain, rest, and to raise poppy. It is the hub or narcotics in Helmand.

- There is still much hard fighting left to do, there are still improvements to be made in the Afghan security capacity, but progress is steady.

- The Corps remains committed to the mission in Regional Command Southwest.

- The contribution and sacrifice of UK troops to the war in Afghanistan is certainly recognized and appreciated here, and Marine commanders on the ground in Afghanistan have publicly recognized that British forces did an excellent job in Sangin, an area which has been and continues to be uniquely challenging.

POINTS OF CONTACT

Capt. Brian Block, HQMC Media Branch, (b)(6)

From: Mclaughlin LtCol Matthew P
To: Mclaughlin LtCol Matthew P
Subject: Wikileaks on UK in Afghanistan
Date: Friday, December 3, 2010 8:44:14 AM
Attachments: 101203 - Wikileaks - British failure in Helmand.doc

---

PA Community,

Pls see this wikileaks related media card/ FRAGPAG and share with your leaders as appropriate.

VR LtCol McLaughlin

From: Yoo BGen Daniel D
To: Armistead Maj Michael W
Cc: Verderame Capt Domenico
Subject: RE: Q&A for the General - March 20
Date: Monday, March 19, 2012 8:16:20 PM

As always, GTG, end of msn. Thx.

V/RS -- DDY

-----Original Message-----
From: Armistead Maj Michael W
Sent: Monday, March 19, 2012 16:48
To: Yoo BGen Daniel D
Cc: Verderame Capt Domenico
Subject: RE: Q&A for the General - March 20

General,

Suggested responses to the below questions as directed.
Responses were based on the excerpts from the following documents:

-BGen Yoo: Philosophy of Command
-FMFM 1-0 Leading Marines
-Commandant's Planning Guidance
-CMC's 2012 report to Congress on the Posture of the Marine Corps (attached)
-USSOCOM's website -Ft Mead press release on MARFORCYBERCOM -JSOU Report 08-1 "Is leaving the Middle East a Viable Option" (attached)

r/

Maj Mike Armistead
Director, Public Affairs
MCRD San Diego/Western Recruiting Region
(b)(6)

-----Original Message-----
From: Yoo BGen Daniel D
Sent: Monday, March 19, 2012 8:37
To: Armistead Maj Michael W
Subject: FW: Q&A for the General - March 20

V/RS -- DDY

-----Original Message-----
From: Verderame Capt Domenico
Sent: Thursday, March 15, 2012 11:07
To: Yoo BGen Daniel D
Subject: FW: Q&A for the General - March 20

General,
FYI Q&A that will be asked to the panel at the Activation Executive Summit.
R/,
Capt Verderame

-----Original Message-----
From: (b)(6)
Sent: Thursday, March 15, 2012 10:21
To (b)(6) Verderame
Capt Domenico
Cc: (b)(6)
Subject: Q&A for the General - March 20

All: Good afternoon. Please see below regarding the panel on March 20.
(b)(6)

From: (b)(6)
Sent: Thursday, March 15, 2012 12:38 PM
To (b)(6)
Subject: FW: Q&A for the General

FYI

From: (b)(6)
Date: Thu, 15 Mar 2012 09:36:37 -0700
To:
Cc: (b)(6)
(b)(6)
Subject: Q&A for the General

Hello (b)(6)

My name is (b)(6) and I head up Strategy and Talent for Activision Blizzard. I was on a call with the General and (b)(6) regarding the upcoming speaking engagement for the General on Tuesday March 20. I wanted to follow up with the questions that (b)(6) will ask the General and the Military Panel, and also to give you some background on the event and what the General can expect.

Background:

This is an internal only event. It bring the top 120 execs from Activision Blizzard worldwide. We are there to listen to top leaders on their thoughts on leadership, building teams and talent, and perspectives about the world

around us. There is no audio or video taping, no outside reporters, etc. The Panel is the General, plus three other Military speakers that were selected by the General. (b)(6) will be the one asking the questions. As you will see, they are open ended to encourage dialogue among the speakers.

Questions: Building Talent - Military Leaders

. Broad outlook

o What is your view of leadership? How does that differ outside of the military?

o How does the military produce/build leaders?

. Building talent

o What makes a Marine?

o How do you build a talented org from the bottom up (i.e. through training programs, recruiting)?

o How is building/retaining talent different for elite teams (e.g. Seal Team Six)?

. Maintaining talent/culture

o How to maintain culture when dispersed across the world?

o How to maintain morale when in a long-term engagement?

o Regarding CODE's big initiative in bringing veterans back to the work force, how does the military help veterans adjust to civilian life?

. Gaming-specific

o How do you view games like Call of Duty?

. Military outlook

o What do you worry about from a security/foreign policy perspective?

o Importance of tech in warfare? How does the U.S. keep its edge?

o Given hacking and security breaches (e.g. Wikileaks), how do we keep secrets in a digital age?

o What are your views on Middle East today from a foreign policy perspective?

Please feel free to call or email me if you have any questions or concerns.

(b)(6)

Chief Strategy and Talent Officer

Activision Blizzard
3100 Ocean Park Blvd

Santa Monica, CA 90405

(b)(6)

Marine Corps Insider Threat

Insider Threat Program Update

17 Aug, 2018

Insider Threat Program Manager

POC: (b)(6)
Program Manager
HQMC PP&O, PS, PSI
(b)(6)

Opening Remarks

- Opening Remarks:
  - Mr. Randy R. Smith (SES) DC Plans Policy Operations (Security)

- Introductions:
  - (b)(6) PP&O Insider Threat Program Manager
  - (b)(6) MCISRE Insider Threat Program Manager
  - Insider Threat Team Members
  - Working Group Attendees

- **WHY ARE YOU HERE??**

Goals/ Agenda

- Provide Program Update and Overview
- Understanding of the requirements
- Establish Stakeholder SME/POCs
- Develop Battle Rhythm
- Direct engagement in policy development
- Assistance in developing processes for information sharing, protection, and utilization
- Identification of gaps in policy and procedure that can be reduced
- How do we help each other???

Philosophical Underpinnings

"The purpose of the MCInTP is to enhance commanders' risk management decisions."

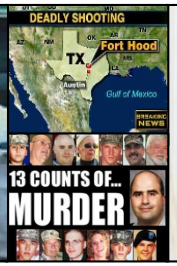
- Marine Corps Bulletin 5510, Marine Corps Insider Threat Program, dated 29 Sep 17

FOCUS ⟶  

- Leadership assisted by technology
- Education and awareness
- Leverage/integrate existing programs
- Crawl, walk, run

- Goal is to be a resource to commanders, not a burden

Events Prompting Policy



2009 Fort Hood

Major Nidal Malik Hasan, an Army officer (psychiatrist) with authorized access to an Army installation, opened fire and killed 13 people and wounded 43 others. The gunman was shot and wounded by responding police officers. Hasan was prosecuted and sentenced to death.

2010 WikiLeaks

Private Chelsea (formerly Bradley) Manning, a U.S. Army soldier, leaked classified and unclassified but sensitive military and diplomatic documents to WikiLeaks. Manning was arrested in May 2010 and convicted in July 2013 of violations of the Espionage Act and sentenced to 35 years imprisonment.

2012 CIA Leak

John Kiriakou, a former CIA analyst and case officer and a senior investigator for the Senate Foreign Relations Committee, pleaded guilty to disclosing classified information about a fellow CIA officer that connected the covert operative to a specific operation. He was the first CIA officer to be convicted for passing classified information to a reporter, although the reporter did not publish the name of the operative. Kiriakou was sentenced to 30 months in prison.

2013 NSA Leak

Edward Snowden, a defense contractor, compromised and leaked highly classified and extremely sensitive intelligence documents. The theft has been described as the most massive and most damaging compromise of intelligence information in our nation's history. Snowden has been charged with two counts of violating the Espionage Act and theft of government property and is allegedly living in an undisclosed location in Russia while seeking asylum elsewhere.

2013 Washington Navy Yard

Aaron Alexis, a defense contractor, opened fire and killed 12 people and wounded three others. Alexis was killed by responding police officers. It was the second-deadliest mass murder on a U.S. military base, behind only the Fort Hood shooting.

2014 Fort Hood

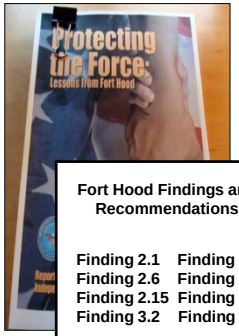
Specialist Ivan Lopez, an Army soldier, opened fire and killed three people and wounded 14 others. Specialist Lopez died of a self-inflicted gunshot wound.

Insider. Any person with authorized access to any United States Government resource to include personnel, facilities, information, equipment, networks and systems. *(National Insider Threat Policy, November 21, 2012)*

Insider threat. The threat an insider will use her or his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities. *(DODD 5205.16, DoD Insider Threat Program)*

Foundational Policies

2009 Fort Hood



Fort Hood Findings and Recommendations

Finding 2.1 Finding 2.5
Finding 2.6 Finding 2.8
Finding 2.15 Finding 2.16
Finding 3.2 Finding 3.7

MCO 5580.3

Violence Prevention Program

December 01, 2012

2010 WikiLeaks

THE WHITE HOUSE

WASHINGTON

October 07. 2011

Executive Order 13587

National Policy

Minimum Standards

November 21, 2012

Dep Sec Defense

Prevention, Assistance, Response Memo

February 2,, 2017

2012 CIA Leak

SECNAVINST 5510.37

Department of the Navy Insider Threat Program

August

DODD 5205.16

DoD Insider Threat Program

September 30, 2014

MCBUL 5510

INSIDER THREAT PROGRAM

September 29 2017

2013 NSA Leak

Mitigation Oversight Task Force (MOTF)

2013 Washington Navy Yard

DoD Insider Threat Management and Analysis Center (DITMAC)

DODD 5205.16 ch1

January 25, 2017

2014 Fort Hood

Policy and Scope

EO 13587

"Structural Reforms To Improve the Security of **Classified Networks** and the Responsible Sharing and Safeguarding of **Classified Information**"

"National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs"

- **Insider**: **Any person with authorized access to any United States Government resource** to include personnel, facilities, information, equipment, networks or systems.

Section 951, FY18 NDAA

- **Insider Threat. A threat presented by a person who *has, or once had, authorized access to information, a facility, a network, a person, or a resource* of the Department**; and wittingly, or unwittingly, commits an act in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities; or ***a destructive act, which may include physical harm to another in the workplace***.

Insider Threat Population

(b)(5)

Requirements

- EO 13587, EO 13526, National InT Minimum Standards
  - 26 Minimum Standards for all DoD Components to establish program and capability

- DoDD 5205-16 DoD Insider Threat Program:

Establish or maintain a multi-disciplinary threat management capability to conduct and integrate the monitoring, analysis, reporting, and response to insider threats. Establish procedures for a multi-disciplinary threat management capability that:

  - Includes the ability to share relevant LE, civilian and military personnel management, mental health, cybersecurity, security, and CI information with commanders (or civilian equivalents) Component-wide.
  - Facilitate timely, informed decision-making by ensuring the following subject matter expertise and multi-disciplinary capabilities are readily available to all commanders (or civilian equivalents):
    - LE, CI, Mental health, Security, Civilian and military personnel management, Legal, Cybersecurity.
    - Echoed by Navy via SECNAVINST. 5510.37 Navy Insider Threat Program

Requirements

- Create an analysis center
- Establish information sharing capability of relevant information
- Cooperate with DoD's analysis center (DITMAC)
- Partner with other service branches
- "Detect, deter, and mitigate insider threats"

Program Alignment

(b)(5)

Program Alignment

(b)(5)

Program Status

(b)(5)

Program Status

(b)(5)

- Develop User Activity Monitoring (UAM) on at least one classified network.
- Provide employee notification of monitoring (i.e. warning banner on Information Systems).

(b)(5)

(b)(5)

- Conduct self-assessments.

Page 41 redacted for the following reason:
- - - - - - - - - - - - - - - - - - - -
(b)(5), (b)(7)(E)

Why we need you

- Policy Expertise
- Training and Education
- Strategic Messaging
- Information Sharing and Protection
- Developing measures of success and effectiveness
- Program Monitoring and Improvement
- Oversight
- Senior Leader Engagement and Investment
- Empowerment and Engagement of Commanders

Approach

- Team approach to the developing policy, the program, and the MCO for Insider Threat
- Goal is to work with each stakeholder individually, to determine:
  - What information or capability exists that can be leveraged to meet the needs of the program
  - How do we share, protect, integrate, segregate the information
  - Legal, ethical, policy concerns
  - Challenges
  - Obstacles

Next Steps

(b)(5)

Closing Information

- Program will begin to make strides towards IOC and FOC as the MCITWG guides the development of policy and procedures, as resources are obtained, and structure in place.
- Crawl, walk, run approach is being taken to ensure efficiency in process development and staffing.
  - (This meeting is our first real step in the walk phase.)

- *The mission cannot be accomplished without your advice, input and support.*

Questions?

From:
To:

(b)(6)

Cc:

Subject: MCITWG 2018
Date: Thursday, August 16, 2018 8:41:12 AM
Attachments: MCITWG 2018 InTP.pdf

Ladies and Gentlemen. The read ahead for tomorrow's Marine Corps Insider Threat Working Group is attached for your review. We look forward to your attendance and the start of our collaboration to establish and implement the National Policy and Minimum Standards for the Marine Corps Insider Threat Program. R/ (b)(6)

Pages 48 through 60 redacted for the following reasons:
- -
(b)(5) - Draft

From:
To:

(b)(6)

Cc:

Subject: MCITWG Charter 20181106
Date: Tuesday, November 6, 2018 1:26:48 PM
Attachments: LOE Revised MCITWG Charter Version 2.0 20181106.docx

---

Good afternoon Ladies and Gentlemen. As (b)(6) briefed during yesterday's MCITWG, we are sending out our MCITWG Charter for an informal review. We request your review, comments, recommendations, and concurrence so we can make any revisions prior to this Charter being placed into DONTRACKER next week for official review. We would appreciate your feedback NLT COB 14 November 2018. We request your feedback be provided via email to (b)(6) Thank You for your assistance and support for our program. R/ (b)(6)

Pages 62 through 74 redacted for the following reasons:
- -
(b)(5) - Draft

From: (b)(6)
To: Armistead LtCol Michael W; (b)(6)
Subject: MCITWG Charter (DON Tracker O6 Level Review)
Date: Thursday, December 27, 2018 9:18:18 AM
Attachments: TAB A MCITWG Charter Version 2.1 20181218 (1).docx

---

RE: Marine Corps Insider Threat Working Group Charter (Policy)

Gentlemen,
I've conducted the review for the subject DON Tracker. Since CommOps and FDR are both providing SME support, we'll have to continue to determine which SME should attend as agenda's are sent prior to convening. certain be will
Key takeaways:

1. Communication Directorate is updated, vice Office of Marine Corps Communication.
2. Director, CD is chartered as an advisory member. (Participation in the MCITWG will be at the appropriate Action Officer level). No other taskings required of CD as it pertains to the WG which will continue to meet each month.

Recommend (b)(5)

S/f

(b)(6)

Pages 76 through 104 redacted for the following reasons:
- -
(b)(5) - Draft

MCO 5510.21, MCCInTP, ENCLOSURE (1), CHAPTER(S) 1-4 (AO REVIEW)							
#	CLASS	COMPONENT AND POC NAME, PHONE, AND E-MAIL	PAGE	PARA	COMMENT TYPE	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	A/R/P

HOW TO USE THE SD FORM 818

GENERAL GUIDANCE:

- **To sort the table** by page number, hover your mouse over the top of the first cell in the column until a downward arrow appears; click to select the entire column. Under Table Tools, select Layout, and then click Sort and "OK." **To add new rows,** copy and paste a blank row to keep consistent formatting. **To add automatic numbering to column 1**, select the entire column and then click on the Numbering button under Paragraph on the Home ribbon.

IF YOU ARE THE COORDINATING OSD COMPONENT:

- Use this form to provide critical and substantive comments to the OSD Component that created the issuance. Complete the header and footer, columns 2-6, and the first two entries in column 7:

COLUMN 1 — Order comments by the pages/paragraphs that they apply to in columns 4 and 5.

COLUMN 2 — Enter the classification of the comment. If any material is **classified**, follow DoDM 5200.01 guidance for marking the document. If all comments are unclassified, mark the header and footer and ignore the column.

COLUMNS 3, 4, AND 5 — Enter the appropriate information for **each** comment.

COLUMN 6 — Enter comment type (C, S, or A).

(C) CRITICAL: When a Component has one or more critical comments, that Component's coordination is an automatic nonconcur. The justification for critical comments MUST identify violations of law or contradictions of Executive Branch or DoD policy; unnecessary risks to safety, life, limb, or DoD materiel; waste or abuse of DoD appropriations; or imposition of an unreasonable burden on a Component's resources.

(S) SUBSTANTIVE: Make a substantive comment if a part of the issuance seems unnecessary, incorrect, misleading, confusing, or inconsistent with other sections, or if you disagree with the proposed responsibilities, requirements, or procedures. One substantive comment is usually not sufficient justification for a nonconcur on an issuance. Multiple substantive comments may be grounds for a nonconcur.

(A) ADMINISTRATIVE: An administrative comment concerns nonsubstantive aspects of an issuance, such as dates of reference, organizational symbols, format, and grammar.

COLUMN 7 — Place only one comment per row. Enter your comment, recommended changes, and justification in the first two areas provided. If any material is **classified**, follow DoDM 5200.01 guidance for marking the document. YOU MUST PROVIDE CONVINCING SUPPORT FOR CRITICAL COMMENTS IN THE JUSTIFICATION.

- **Review** the comments, **resolve** any conflicting views, and **confirm** that the completed matrix accurately represents your Component's position. Upload the form to the DoD Directives Program Portal in **Microsoft Word format (.docx)**, with the signed SD Form 106 or coordination memorandum.

IF YOU ARE THE ORIGINATING OSD COMPONENT:

- Consolidate comments from all coordinators and adjudicate them. **DO NOT include coordinator's administrative comments** in the consolidated SD 818. Leave columns 4 and 5 blank for general comments that apply to the whole document. **Sort comments** by the pages/paragraphs to which they apply using the **General Guidance** sort feature (e.g., all comments from all coordinators that apply to page 1, paragraph 1.a., should be together; all comments that apply to page 1, paragraph 1.b., should be next). Set classification header, footer, and columns 1 and 2 as appropriate. Complete last entry in column 7, and column 8:

COLUMN 7 — If you rejected or partially accepted a comment, enter your justification in the originator justification area. If any material is **classified**, follow DoDM 5200.01 guidance for marking the document. Leave blank if you accepted it. Include any related communications with the coordinating Component. You MUST provide convincing support for rejecting critical comments.

MCO 5510.21, MCCInTP, ENCLOSURE (1), CHAPTER(S) 1-4 (AO REVIEW)							
#	CLASS	COMPONENT AND POC NAME, PHONE, AND E-MAIL	PAGE	PARA	COMMENT TYPE	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	A/R/P

COLUMN 8 Enter whether you accepted (A), rejected (R), or partially accepted (P) the comment. Your justification in column 7 must be consistent with this entry.

	Choose an item.				Choose an item.	**Coordinator Comment:** **Coordinator Justification:** **Originator Justification for Resolution:**	Choose an item.
	Choose an item.				Choose an item.	**Coordinator Comment:** **Coordinator Justification:** **Originator Justification for Resolution:**	Choose an item.
	Choose an item.				Choose an item.	**Coordinator Comment:** **Coordinator Justification:** **Originator Justification for Resolution:**	Choose an item.
	Choose an item.				Choose an item.	**Coordinator Comment:** **Coordinator Justification:** **Originator Justification for Resolution:**	Choose an item.
	Choose an item.				Choose an item.	**Coordinator Comment:** **Coordinator Justification:** **Originator Justification for Resolution:**	Choose an item.

MCO 5510.21, MCCInTP, ENCLOSURE (1), CHAPTER(S) 1-4 (AO REVIEW)							
#	CLASS	COMPONENT AND POC NAME, PHONE, AND E-MAIL	PAGE	PARA	COMMENT TYPE	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	A/R/P

Marine Corps Counter-Insider Threat Working Group (MCCITWG)

Office	Name	Rank	
PP&O PS	Mr. Randy R. Smith	SES	Assistant Deputy Commandant, Plans, Policies, and Operations (Security)/Senior Official for the Marine Corps Counter-Insider Threat Program (MCCInTP)
PP&O PS	(b)(6)		Security Division Deputy Director
PP&O PS PSI			Identity Activities Branch Head
PP&O PS PSI			MCInTP Manager (Acting)
PP&O PS PSL			Deputy Branch Head (PSL)
PP&O PS PSL			Plans and Policy Officer
PP&O PS PSP			AT Program Manager
PP&O PLI			Branch Head
PP&O PLI			OPSEC PM
HQMC CL			Associate Counsel, CL
HQMC CL			Associate Counsel, CL

(b)(6)

HQMC JAD	(b)(6)	International and Operational Law Branch Head	(b)(6)
HQMC JAD		International and Operational Law Deputy Branch Head	
HQMC G-10		Operations Officer	
HQMC HS		Executive Assistant to the Medical Officer of the Marine Corps	
HQMC HS		Director of Public Health	
HQMC Privacy ARSF		USMC Privacy Program Coordinator	
HQMC FOIA ARSF		Deputy FOIA PA	
IGMC		Intelligence Oversight	
IGMC		Executive Assistance	
CMC SD		Deputy Director	
CMC SD		Branch Head, Ground Branch	
DC P&R			

DC I	(b)(6)	Plans and Strategy Division	(b)(6)
DC I 4B655		Plans and Strategy Division	
C4/CY		Cyber Security Analyst	
C4/CY		Privacy Analyst	
HQMC-I		Chief of Staff	
HQMC - I		Counterintelligence Policy Chief	
HQMC - I		Ground Intelligence Chief	
HQMC - I		DEO CI/HUMINT Branch	
HQMC - I		Assistant Special Security Officer (ASSO)	
MCISRE InTP		MCISRE/I Dept Insider Threat Program Manager	
MCISRE InTP		MCISRE/I Dept Insider Threat Senior Analyst	
MCISRE InTP		MCISRE/I Dept Insider Threat Social Scientist	
MCIA M2X			
MCIA SJA		Command Judge Advocate	

Office	Name	Rank	Billet	Contact #	NIPR	SIPR
MP Division MPC	(b)(6)		Supervisor, Civilian Workforce Planning & Development Section MPC-30	(b)(6)		
MPP-10			Future Operations Manpower Plans & Policy			
MI			Action Officer			
MMIB			MMIB Branch Head MM Division CIO			
MMIB			MMIB Operations Analyst MM Division Asst CIO			
DC M&RA			Physical Security Office			
MF			Marine & Family Programs			
MF			Marine & Family Programs			
MF			Marine & Family Programs			
MF			Marine & Family Programs			
DC AVN			ASM (Future APP 1-B)			
DC AVN			APP 2			

Office			
CDD, FPID	(b)(6)	Branch Head LE/EOF	(b)(6)
CDD, FPID		Deputy Branch Head LE/EOF	
CDD, FPID		Program Analyst	
TECOM G-3/5/7 Support Branch		Mission Assurance Program Manager & Antiterrorism Officer	
TECOM Security Directorate		Command Security Manager	
DC I&L		LPV-2 Deputy Section Head Log Systems Technology & Integration	
MCICOM G-3		Director of Operations	
MCICOM G-3		Deputy Director of Operations	
MCICOM G-3		Head of Law Enforcement and Security	
MCICOM G-3		LE Analyst	

Office			
MCRC	(b)(6)	Mission Assurance Officer	(b)(6)
MCRC		Deputy COS G-4	
MCSC		Assistant Chief of Staff, G-2 (Security)	
MCSC		Physical Security - AT/FP Officer	
Communication Directorate		Force Development and Requirements Branch	
Communication Directorate		Force Development and Requirements Branch	
Communication Directorate		Communication Ops	
MCB Quantico		Threat Assessment Officer	

Office		Billet	Contact #	NIPR	SIPR
MARFORCYBER G2X	(b)(6)	G2X Officer-in-Charge		(b)(6)	
MARFORCYBER Future Operations		DCO OPT Team Leader			
MARFORCYBER G-9					
MARFORCYBER Future Operations		DCO			
MARFORCYBER G5					
MARFORCYBER G5					
MCCOG		CSSP Program Manager			
MCCOG					
MCIOC		Integrated Joint Special Technical Operations (IJSTO) Control Officer			

MCCInTP	(b)(6)	Insider Threat Program Support	(b)(6)
MCCInTP		Deputy Program Support	
MCCInTP		Senior Analyst	
MCCInTP		Senior Analyst	
MCCInTP		Senior Analyst	
MCCInTP		Senior Analyst	
MCCInTP		Mid-Analyst	
MCCInTP		Mid-Analyst	
MCCInTP		Mid-Analyst	
MCCInTP		Policy SME	
MCCInTP		Social Scientist	

From:
To:

(b)(6)

Cc:

Subject: Warning Order
Date: Friday, February 8, 2019 12:40:03 PM
Attachments: MCO 5510.21 20190211 Encl 1 Chapter 1 References.docx
MCO 5510.21 20190211 Encl 1 Chapter 2 Acronyms.docx
MCO 5510.21 20190211 Encl 1 Chapter 3 Definitions.docx
MCO 5510.21 20190211 Encl 1 Chapter 4 Background.docx
MCO 5510.21 SD-818 AO CRM for Chapter 1 through 4.docx
MCITWG Validated Membership Roster 20190206.pptx

Good afternoon Ladies and Gentlemen. Let me first wish you all a restful and safe weekend.

Attached are Chapters 1-4 supporting MCO 5510.21.

These Chapters will be loaded into DONTRACKER on Monday for your official comments/concurrence/nonconcurrence.

This is just an advanced copy of the DONTRACKER to get ahead of the process.

These Chapters (15) in all will come out fast and furious.

The Basic Order will also come out on DONTRACKER in parallel.

We appreciate your assistance in getting our Order moving forward.

Note: There are a lot of references, please validate your references are included or if there are others that would better support your program please add to the CRM.

My best to all...

R (b)(6)

Pages 117 through 136 redacted for the following reasons:
- -
(b)(5) - Draft

MCO 5510.21, MCCInTP, ENCLOSURE (1), CHAPTER(S) 1-4 (AO REVIEW)							
#	CLASS	COMPONENT AND POC NAME, PHONE, AND E-MAIL	PAGE	PARA	COMMENT TYPE	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	A/R/P

HOW TO USE THE SD FORM 818

GENERAL GUIDANCE:

- **To sort the table** by page number, hover your mouse over the top of the first cell in the column until a downward arrow appears; click to select the entire column. Under Table Tools, select Layout, and then click Sort and "OK." **To add new rows,** copy and paste a blank row to keep consistent formatting. **To add automatic numbering to column 1**, select the entire column and then click on the Numbering button under Paragraph on the Home ribbon.

IF YOU ARE THE COORDINATING OSD COMPONENT:

- Use this form to provide critical and substantive comments to the OSD Component that created the issuance. Complete the header and footer, columns 2-6, and the first two entries in column 7:

COLUMN 1 — Order comments by the pages/paragraphs that they apply to in columns 4 and 5.

COLUMN 2 — Enter the classification of the comment. If any material is **classified**, follow DoDM 5200.01 guidance for marking the document. If all comments are unclassified, mark the header and footer and ignore the column.

COLUMNS 3, 4, AND 5 — Enter the appropriate information for **each** comment.

COLUMN 6 — Enter comment type (C, S, or A).

(C) CRITICAL: When a Component has one or more critical comments, that Component's coordination is an automatic nonconcur. The justification for critical comments MUST identify violations of law or contradictions of Executive Branch or DoD policy; unnecessary risks to safety, life, limb, or DoD materiel; waste or abuse of DoD appropriations; or imposition of an unreasonable burden on a Component's resources.

(S) SUBSTANTIVE: Make a substantive comment if a part of the issuance seems unnecessary, incorrect, misleading, confusing, or inconsistent with other sections, or if you disagree with the proposed responsibilities, requirements, or procedures. One substantive comment is usually not sufficient justification for a nonconcur on an issuance. Multiple substantive comments may be grounds for a nonconcur.

(A) ADMINISTRATIVE: An administrative comment concerns nonsubstantive aspects of an issuance, such as dates of reference, organizational symbols, format, and grammar.

COLUMN 7 — Place only one comment per row. Enter your comment, recommended changes, and justification in the first two areas provided. If any material is **classified**, follow DoDM 5200.01 guidance for marking the document. YOU MUST PROVIDE CONVINCING SUPPORT FOR CRITICAL COMMENTS IN THE JUSTIFICATION.

- **Review** the comments, **resolve** any conflicting views, and **confirm** that the completed matrix accurately represents your Component's position. Upload the form to the DoD Directives Program Portal in **Microsoft Word format (.docx)**, with the signed SD Form 106 or coordination memorandum.

IF YOU ARE THE ORIGINATING OSD COMPONENT:

- Consolidate comments from all coordinators and adjudicate them. **DO NOT include coordinator's administrative comments** in the consolidated SD 818. Leave columns 4 and 5 blank for general comments that apply to the whole document. **Sort comments** by the pages/paragraphs to which they apply using the **General Guidance** sort feature (e.g., all comments from all coordinators that apply to page 1, paragraph 1.a., should be together; all comments that apply to page 1, paragraph 1.b., should be next). Set classification header, footer, and columns 1 and 2 as appropriate. Complete last entry in column 7, and column 8:

COLUMN 7 — If you rejected or partially accepted a comment, enter your justification in the originator justification area. If any material is **classified**, follow DoDM 5200.01 guidance for marking the document. Leave blank if you accepted it. Include any related communications with the coordinating Component. You MUST provide convincing support for rejecting critical comments.

MCO 5510.21, MCCInTP, ENCLOSURE (1), CHAPTER(S) 1-4 (AO REVIEW)							
#	CLASS	COMPONENT AND POC NAME, PHONE, AND E-MAIL	PAGE	PARA	COMMENT TYPE	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	A/R/P

COLUMN 8 Enter whether you accepted (A), rejected (R), or partially accepted (P) the comment. Your justification in column 7 must be consistent with this entry.

	Choose an item.				Choose an item.	**Coordinator Comment:** **Coordinator Justification:** **Originator Justification for Resolution:**	Choose an item.
	Choose an item.				Choose an item.	**Coordinator Comment:** **Coordinator Justification:** **Originator Justification for Resolution:**	Choose an item.
	Choose an item.				Choose an item.	**Coordinator Comment:** **Coordinator Justification:** **Originator Justification for Resolution:**	Choose an item.
	Choose an item.				Choose an item.	**Coordinator Comment:** **Coordinator Justification:** **Originator Justification for Resolution:**	Choose an item.
	Choose an item.				Choose an item.	**Coordinator Comment:** **Coordinator Justification:** **Originator Justification for Resolution:**	Choose an item.

MCO 5510.21, MCCInTP, ENCLOSURE (1), CHAPTER(S) 1-4 (AO REVIEW)							
#	CLASS	COMPONENT AND POC NAME, PHONE, AND E-MAIL	PAGE	PARA	COMMENT TYPE	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	A/R/P

From:
To:

(b)(6)

Cc:

Subject: MCO 5510.21 Virtual MCCITWG
Date: Thursday, February 21, 2019 9:28:13 AM
Attachments: MCO 5510.21 20190221 Encl 1 Ch 1 References.docx
MCO 5510.21 20190221 Encl 1 Ch 2 Acronyms.docx
MCO 5510.21 20190221 Encl 1 Ch 3 Definitions.docx
MCO 5510.21 20190221 Encl 1 Ch 4 Background.docx
MCO 5510.21 SD-818 AO CRM for Chapter 1 through 4.docx

Good morning once again to all.

Attached is enclosure (1) Chapters 1-4 of MCO 5510.21.

These chapters shall be loaded into DONTRACKER for official tasking later this morning.

For clarification purposes, we are aware this is an unconventional approach to staffing an Order.

Our intent is to get the group think tank going as we prepare to staff the basic order.

By providing these few references up front, we believe it shall provide a solid footing for future reviewers when the Order is staffed out for review.

With the references, acronyms, definitions, and background information, we hope they set the tone for successful information sharing as the Directives Review Process begins.

I will send out the official DONTRACKER number to follow-up this email.

Thanks

R/ (b)(6)

Wikileaks

BACKGROUND

New Executive Order entitled "*Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information."* EO was issued Friday Oct 7, 2011. Wikileaks triggered White-House led effort to determine what happened and how to fix it. The new EO is the product of that review. Some press attention has resulted with specific questions regarding Private Manning.

NEW INIATITIVES

- Training our people. Annual DoD training has been updated to emphasize security rules, and that people are accountable. All DoD personnel take that training each year.

- Stopping people from downloading classified data onto removable storage like DVDs, CDs, and removable memory sticks.
  - DoD deployed a tool to essentially every DoD computer to prevent downloads except where explicitly authorized for mission essential exceptions.
  - Tool is called the Host-Based Security System (HBSS), a commercial piece of software that monitors, detects, and counters known cyber-threats.
  - DoD Components report that 87.5 percent of SIPRNET machines are write disabled; 12.5 percent are write-enabled, but under controls that require two-person integrity checks.

- Driving out anonymity and increasing accountability by giving a cyber identity credential to every DoD person and requiring their use on classified networks.
  - DoD has issued a cyber identity credential to every person who uses the unclassified networks
  - This year DoD has begun issuing a similar credential to every person who uses the SIPRNET. Completed in FY-13. Refer questions to DoD CIO.

TALKING POINTS

- The goal is to fix security through coordinated, government-wide efforts to provide uniform protections for classified information while ensuring information can still be shared appropriately.

- We have taken and continue to take steps to prevent such compromises, like Wikileaks, from happening again.

- We're doing this in a way that preserves our commitment to share the information needed by our Marines to accomplish their mission.

- Questions about Private Manning: Due to an ongoing investigation, refer all questions pertaining to Private Bradley Manning to the Army.

POINT OF CONTACT/SOURCING

(b)(6)

From: <The SANS Institute on behalf of The SANS Institute
To: (b)(6)
Subject: SANS NewsBites Vol. 15 Num. 043 : Critical Security Controls Subjected to ROI Analysis; Federal Magistrate Reverses Ruling, Requires Man to Decrypt Storage Devices; Google Cuts Grace Period on Actively Exploited Vulnerabilities to 7 Days; Cyber Retaliation is "A Remarkably Bad Idea"
Date: Friday, May 31, 2013 1:39:04 PM

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

****
SANS NewsBites May 31, 2013 Vol. 15, Num. 043
****

TOP OF THE NEWS

THE REST OF THE WEEK'S NEWS

********** SPONSORED BY Symantec **********

****

TRAINING UPDATE

http://www.sans.org/event/ipv6-summit-2013/course/ipv6-essentials
http://www.sans.org/event/ipv6-summit-2013

- -- SANS Rocky Mountain 2013 Denver, CO July 14-20, 2013
10 courses. Bonus evening sessions include OODA - The Secret to Effective Security in Any Environment; and APT: It is Not Time to Pray, It is Time to Act.
http://www.sans.org/event/rocky-mountain-2013

- -- SANS San Francisco 2013 San Francisco, CA July 29-August 3, 2013
7 courses. Bonus evening sessions include Offensive Digital Forensics; and Base64 Can Get You Pwned!
http://www.sans.org/event/san-francisco-2013

- -- SANS Boston 2013 Boston, MA August 5-10, 2013
9 courses. Bonus evening sessions include Cloud R and Forensics; and You Can Panic Now. Host Protection is (Mostly) Dead.
http://www.sans.org/event/boston-2013

- -- SANS Virginia Beach 2013 Virginia Beach, VA August 19-30, 2013
10 courses. Bonus evening presentations include Thanks for Recovering ... Now I Can Hack You!; Everything I Know is Wrong!; and APT: It is Time to Act.
http://www.sans.org/event/virginia-beach-2013

- -- SANS Pen Test Berlin 2013 Berlin, Germany June 2-June 8, 2013
Europe's only specialist pen test training and networking event. Four dedicated pen test training courses led by five SANS world-class instructors.
http://www.sans.org/event/pentest-berlin-2013

- -- SANS London Summer 2013 London, UK July 9-July 16, 2013
5 courses. SANS has added a new London date to the security-training calendar, giving security professionals the opportunity to take one of four of SANS' most popular 6-day courses and the excellent 2 day Securing The Human course.
http://www.sans.org/event/london-summer-2013

- -- Multi-week Live SANS training
http://www.sans.org/mentor/about
Contact mentor@sans.org

- -- Looking for training in your own community?
http://www.sans.org/community/

- -- Save on On-Demand training (30 full courses) - See samples at
http://www.sans.org/ondemand/discounts.php#current
Plus Malaysia, Canberra, Austin and Mumbai all in the next 90 days.
For a list of all upcoming events, on-line and live: www.sans.org

****

TOP OF THE NEWS
--Analysis: First Return on Investment (ROI) Analysis for the Critical Security Controls
(May 30, 2013)
John Pescatore compares Idaho State University's (ISU) projected cost of settling HIPAA violations with the US Department of Health and Human Services (HHS) to what it would have cost the university to implement security controls that could have (helped) protect its systems from breaches. The estimated cost to ISU, including the fine, the costs of managing the breach, and the implementation of a Corrective Action Plan is US $1 million over two years. Putting in place certain Critical Security Controls that would have detected the issue that exposed patient data would cost an estimated US $75,000. Even adding in extras like vulnerability assessments and monitoring would put the cost at US $500,000, equivalent to one year's share of the above cost.
http://www.sans.org/security-trends/2013/05/30/analyzing-the-cost-of-a-hipaa-related-breach-through-the-lens-of-the-critical-security-controls

--Federal Magistrate Reverses Ruling, Requires Wisconsin Man to Decrypt Storage Devices

(May 28, 2013)

US Magistrate William Callahan Jr. has ordered a Wisconsin man suspected of possessing child pornography to decrypt hard drives that law enforcement authorities seized from his home. In early April, Callahan ruled that to order Jeffrey Feldman to decrypt the devices would be a violation of his Fifth Amendment rights. At that time, prosecutors had been unable to crack the encryption on any of the devices. But since that ruling, prosecutors managed to decrypt a portion of one of the devices and found content linking Feldman to them. So Callahan reversed his order, writing, "the government has now persuaded me that it is a 'foregone conclusion' that Feldman has access to and control over the subject storage devices" and that "Fifth Amendment protection is no longer available to" the defendant. Callahan has ordered Feldman to either provide prosecutors with the passwords necessary to decrypt the data storage devices or provide decrypted copies of everything on those drives.

http://www.wired.com/threatlevel/2013/05/decryption-order/

http://www.computerworld.com/s/article/9239612/Decryption_disclosure_doesn_t_violate_Fifth_Amendment_judge_rules_in_child_porn_case?taxonomyId=17

http://www.wired.com/images_blogs/threatlevel/2013/05/decryptorder.pdf

[Editor's Note (Pesctore): Court decisions have generally gone this way, dating back to the days of the courts recognizing that people should be required to open safes or locked lockers harboring physical evidence. (Northcutt): Several similar cases are floating through the legal system. Here are a couple more links on the topic, but keep in mind these are from journalists, not legal scholars. Apparently the Washington Post author is not familiar with Boucher, the first case in this genre. The cryptome analysis is the best I have found to date:

http://www.washingtonpost.com/wp-dyn/content/article/2008/01/15/AR2008011503663.html

http://www.forbes.com/sites/andygreenberg/2012/02/24/two-cases-lessons-if-cops-dont-know-what-you-encrypted-they-cant-make-you-decrypt-it/

http://cryptome.org/isp-spy/crypto-spy.pdf

Also keep in mind that while child pornography and terrorism are abhorrent and inexcusable, the case law being established will apply to other unrelated use cases like divorce, tax evasion and even potentially traffic accidents:

http://www.wired.com/autopia/2013/02/russian-dash-cams/]

--Google Cuts Grace Period on Actively Exploited Vulnerabilities to Seven Days

(May 29 & 30, 2013)

Google has announced that it will give software vendors whose products are being actively exploited just seven days to issue a fix or an advisory that includes workarounds or other mitigation suggestions. After the week-long grace period, the company said it would make details of the flaw public in such a way as to allow users to protect their systems. Prior to the announcement, Google gave vendors 60 days before going public. Google acknowledges that its new stance is "aggressive," but maintains that one week is sufficient time to release risk mitigation advice. Google says it will abide by the same requirements to address bugs in its own products.

http://www.darkreading.com/vulnerability/google-sets-new-aggressive-7-day-deadlin/240155757

http://www.zdnet.com/google-security-flaws-not-fixed-in-a-week-should-be-made-public-7000016124/

http://www.h-online.com/security/news/item/Google-cuts-grace-period-for-vendors-of-vulnerable-software-1873878.html

http://googleonlinesecurity.blogspot.com/2013/05/disclosure-timeline-for-vulnerabilities.html

[Editor's Note (Pescatore): Making the software vendors feel more pain has over time proven to be a good thing in getting them to invest in better development and patching processes, but I think 7 days is too short for complex software, such as operating systems or databases, or embedded or specialty apps like industrial control systems and the like. Thirty days would make more sense. Pushing out bad mitigation advice quickly is not a great thing.]

--Response: Private Organizations Engaging in Cyber Retaliation is "A Remarkably Bad Idea"

(May 29, 2013)

The Center for Strategic and International Studies (CSIS) has released

commentary responding to a recently released report from the Commission on the Theft of American Intellectual Property suggesting that private organizations be allowed to retaliate against cyberthieves. James Lewis, senior fellow and director of the technology and public policy program at CSIS, wrote, "Our goal is to make cyberspace more stable and secure, not less. Endorsing retaliation works against that goal in many ways, all damaging." The US has been making an effort to build consensus for the idea that "states are responsible for the actions of those resident on their territory and must take action against cybercrime." Furthermore, the US government has backed the Budapest Convention on Cybercrime, under which private retaliation would be a crime.
http://www.computerworld.com/s/article/9239606/Private_retaliation_in_cyberspace_a_remarkably_bad_idea_?taxonomyId=17
http://csis.org/publication/private-retaliation-cyberspace
[Editor's Note (Murray): Vigilantes are thugs who have abandoned the Rule of Law and are not entitled to its protections.
(Honan): It astounds me how people in companies that cannot protect their own systems think they have the skills to identify and retaliate against their attackers.
(Shpantzer): There's a lot of room between doing nothing and 'retaliation.' See some of Dave Dittrich's thoughts (book coming soon) here http://www.honeynet.org/node/1004.]

********** Sponsored Links: **********

****

THE REST OF THE WEEK'S NEWS

--Known Flaw in Ruby on Rails is Being Actively Exploited
(May 28, 29, & 30, 2013)
A known vulnerability in the Ruby on Rails web application framework is being exploited to force unpatched servers into joining a botnet. A patch for the flaw has been available since January, but the success of recent exploits suggests that the patch has not been widely installed. Users are urged to make sure that the versions of Ruby on Rails that they are running are 3.2.11, 3.1.10, 3.0.19, 2.3.15 or later. If updating immediately is not an option, users can also employ workarounds to protect their servers.
http://www.zdnet.com/ruby-on-rails-flaw-being-used-to-recruit-servers-in-botnets-7000016117/
http://www.theregister.co.uk/2013/05/30/rails_botnet_threat/
http://arstechnica.com/security/2013/05/critical-ruby-on-rails-bug-exploited-in-wild-hacked-servers-join-botnet/
http://www.computerworld.com/s/article/9239588/Hackers_exploit_Ruby_on_Rails_vulnerability_to_compromise_servers_create_botnet?taxonomyId=17
http://weblog.rubyonrails.org/2013/1/8/Rails-3-2-11-3-1-10-3-0-19-and-2-3-15-have-been-released/

--PayPal Fixes Cross-Site Scripting Flaw, Defends Decision Not to Award Teen Bug Bounty
(May 30, 2013)
PayPal has fixed a cross-site scripting (XSS) hole security in its portal that could have been exploited to steal users' access information. The flaw allowed attackers to inject JavaScript code into the site; the vulnerability had been public for five days before it was addressed. The flaw was disclosed by a 17-year-old, who was denied

participation in PayPal's bug bounty program because he was not yet 18. He gave the company a week before he released details of the vulnerability. The teen says he later received a message from PayPal notifying him that someone else had informed the company about the issue earlier then he had.
http://www.h-online.com/security/news/item/PayPal-vulnerability-finally-closed-1873322.html
http://www.theregister.co.uk/2013/05/30/paypal_bug_bounty/
[Editor's Note (Murray): "Cross-site scripting" is an attack, not a "hole." The hole, or vulnerability is incomplete parameter checking. The practice, no matter how popular and common, of naming vulnerabilities for the attacks that exploit them perpetuates the coding practices that lead to the vulnerability. Complete parameter checking is difficult at best, requires special knowledge and skill, and must be done at every layer; it cannot all be done in the application layer. The requisite knowledge and skill is not being taught, recognized, or rewarded. The result is that instances of successful SQL injection attacks, cross-site scripting, buffer over-flows, and other attacks that exploit incomplete parameter checking persist or increase.]

--Drupal Resets Passwords After Breach
(May 29 & 30, 2013)
Drupal.org has reset all account passwords after discovering that intruders had gained unauthorized access to information on its servers. The intrusion was made through unspecified third-party software on the organization's servers. Nearly one million accounts are affected.
http://www.h-online.com/security/news/item/Drupal-org-compromised-1873388.html
http://www.zdnet.com/drupal-issues-password-reset-after-servers-compromised-7000016067/
http://arstechnica.com/security/2013/05/drupal-org-resets-login-credentials-after-hack-exposes-password-data/
http://www.computerworld.com/s/article/9239613/Drupal_resets_account_passwords_after_detecting_unauthorized_access?taxonomyId=17

--Chinese Military Drill to Include Digital Warfare Exercises
(May 29, 2013)
In late June, China's People's Liberation Army "will conduct an exercise ... to test new types of combat forces including units using digital technology amid efforts to adjust to informationalized war." According to Chinese news agency Xinhua, the PLA says that the exercise will be the first time it "has focused on combat forces including digitalized units, special operations forces, army aviation, and electronic counter forces."
http://www.zdnet.com/cn/chinese-army-to-include-digital-forces-in-june-military-drill-7000016008/
http://www.theatlanticwire.com/technology/2013/05/china-cyberwar-drill/65678/
http://news.cnet.com/8301-1009_3-57586569-83/chinas-military-to-train-on-digital-warfare/

--FTC Asks Judge to Reject Wyndham Hotels' Motion to Dismiss Complaint
(May 29, 2013)
The US Federal Trade Commission (FTC) has filed documents asking a US District Court to toss out Wyndham Hotels' motion to dismiss an FTC complaint against the company after it suffered a number of data security breaches. Wyndham argued that the FTC is exceeding its authority because it is trying to make cybersecurity issues into consumer protection issues, saying the FTC "wants to turn a statute designed to protect consumers from unscrupulous businessmen into a tool to punish businesses victimized by criminals." But court documents say "the FTC is not suing Wyndham for the fact that it was hacked, it is suing Wyndham for mishandling consumers' information such that hackers were able to steal it." The case is significant because "in the absence of comprehensive cybersecurity legislation ... the only effective method for cybersecurity regulation by the government is to use the FTC's enforcement authority."
http://www.scmagazine.com/wyndham-hotels-court-battle-over-ftc-data-security-authority-heats-up-again/article/295397/
http://www.lawfareblog.com/2013/05/the-most-important-cybersecurity-case-youve-never-heard-of/
[Editor's Note (Pescatore): There is actually a lot of existing legislation that allows multiple government agencies to go after companies that expose privacy-related information. HHS has finally started to take enforcement actions, FTC has been a shining example. The issue has not been lack of legislation; it has been lack of enforcement. I'm hoping the courts do agree that businesses that fail to take basic precautions to protect their customer's personal information are indeed "unscrupulous."]

--Jeremy Hammond Pleads Guilty to Stratfor Data Theft
(May 28 & 29, 2013)
Jeremy Hammond has pleaded guilty to a number of charges, including hacking and conspiracy to commit access device fraud, for stealing data from global intelligence company Stratfor, which counts the US Department of Defense, Lockheed Martin, and Bank of America among its clients. The stolen data included credit card information and more than five million email messages. Some of the messages have been published by WikiLeaks, and some of the compromised credit card accounts were used to make US $700,000 in fraudulent charges. Hammond told the judge that in each case, he "knew what [he] was doing was against the law." Hammond is allegedly a member of a hacking group that has ties to Anonymous.
http://news.cnet.com/8301-1009_3-57586787-83/hacker-accused-of-massive-stratfor-attack-pleads-guilty/
http://www.bbc.co.uk/news/technology-22703579
http://www.wired.com/threatlevel/2013/05/hammond-plea/
http://www.informationweek.com/security/attacks/anonymous-hacker-jeremy-hammond-pleads-g/240155718

--Harvard College Dean Who Authorized eMail Searches Stepping Down
(May 28, 2013)
The Harvard College dean who authorized secret searches of residential deans' email messages will step down this summer. Evelynn M. Hammonds acknowledged that she authorized the searches, which were aimed at identifying the source of an information leak about a cheating scandal that emerged at the school in 2012. Hammonds and other administrators maintained that automated searches were made only of email subject lines to determine who had shared a confidential message with someone at the Harvard Crimson newspaper, and that the searches were conducted in an effort to protect the privacy of the students involved in the cheating scandal. The administrators also acknowledged that it was a mistake not to notify the deans of the search either before or after the fact.
http://www.computerworld.com/s/article/9239574/Harvard_dean_who_okayed_secret_faculty_email_search_steps_down?taxonomyId=17
http://www.cnn.com/2013/05/28/us/massachusetts-harvard-dean/?hpt=hp_t2

--Texas Legislature Passes Strong eMail Privacy Bill
(May 28, 2013)
Texas state legislators have passed a bill that would require law enforcement officials to obtain a warrant to access all emails, regardless of whether or not they have been opened, and regardless of how old they are. Governor Rick Perry has until June 16 to sign or veto the bill. If he does not take action, it will automatically become law on September 1, 2013. If it does become law, it would be the strongest email privacy law in the country. The law would not affect federal investigations.
http://arstechnica.com/tech-policy/2013/05/unprecedented-e-mail-privacy-bill-sent-to-texas-governors-desk/

****

high schools to the Air Force. He is also author and lead instructor of the SANS Hacker Exploits and Incident Handling course, and Penetration Testing course..

Michael Assante was Vice President and Chief Security Officer at NERC, led a key control systems group at Idaho National Labs, and was American Electric Power's CSO. He now leads the global cyber skills development program at SANS for power, oil & gas and other critical infrastructure industries.

Mark Weatherford is a Principal at The Chertoff Group and the former Deputy Under Secretary of Cybersecurity at the US Department of Homeland Security.

William Hugh Murray is an executive consultant and trainer in Information Assurance and Associate Professor at the Naval Postgraduate School.

Sean McBride is Director of Analysis and co-founder of Critical Intelligence, and, while at Idaho National Laboratory, he initiated the situational awareness effort that became the ICS-CERT.

Rob Lee is the SANS Institute's top forensics instructor and director of the digital forensics and incident response research and education program at SANS (computer-forensics.sans.org).

Tom Liston is a Senior Security Consultant and Malware Analyst for InGuardians, a handler for the SANS Institute's Internet Storm Center, and co-author of the book Counter Hack Reloaded.

Dr. Eric Cole is an instructor, author and fellow with The SANS Institute. He has written five books, including Insider Threat and he is a founder with Secure Anchor Consulting.

Mason Brown is one of a very small number of people in the information security field who have held a top management position in a Fortune 50 company (Alcoa). He is leading SANS' global initiative to improve application security.

David Hoelzer is the director of research & principal examiner for Enclave Forensics and a senior fellow with the SANS Technology Institute.

Gal Shpantzer is a trusted advisor to CSOs of large corporations, technology startups, Ivy League universities and non-profits specializing in critical infrastructure protection. Gal created the Security Outliers project in 2009, focusing on the role of culture in risk management outcomes and contributes to the Infosec Burnout project.

Alan Paller is director of research at the SANS Institute.

Brian Honan is an independent security consultant based in Dublin, Ireland.

David Turley is SANS infrastructure manager and serves as production manager and final editor on SANS NewsBites.

-----BEGIN PGP SIGNATURE-----

iEYEARECAAYFAlGo1HAACgkQ+LUG5KFpTkbybQCdG4VtI+1LsEdAADq/YPSe8+VX
qYkAoKAob80d6KhiX9lsrx0uUsTPpISd
=vGJM
-----END PGP SIGNATURE-----

From: Network Management Bulletin
To: (b)(6)
Subject: [EEMSG: Marketing]How to Think Like a Hacker
Date: Sunday, January 25, 2015 9:26:41 AM

Read Online

How to Think Like a Hacker

Robust information marketplaces have arisen for hackers to sell credit card information, account usernames, passwords, national secrets (WikiLeaks), as well as intellectual property. How does anyone keep secrets protected from hackers?

The best way to beat a hacker is to think like one. This paper outlines the five stages hackers use to steal to steal your data and what you can do to prevent it.

Download now

emedia Communications LLC
200 N LaSalle St., Suite 2450, Chicago, IL 60601. USA
Toll free: 800-782-6167
e-mail: inquiries@emedia.com

From:
To: (b)(6)
Cc:
Subject: WikiLeaks
Date: Wednesday, March 8, 2017 12:30:39 PM

To our entire ARI Team

Before we have an incident, I need to address the topic of WikiLeaks to the entire ARI Team/Staff. DO NOT, and I repeat DO NOT under any circumstance access the WikiLeaks site on a MCEN computer or Smartphone. Recent documents posted by WikiLeaks are classified. Any attempt or the successful accessing of this material or any other questionable material on this site will constitute a spillage. Additionally, and while we cannot monitor your surfing activities from a personal device via your cellular carrier or commercial ISP outside the work environment, I would submit accessing this site and viewing any of this material outside the MCEN or work environment would also be unwise as it could impact your clearance.

Your ability to obtain and maintain a secret or top secret clearance is a condition of your employment to work in ARI work spaces, and to perform tasks associated with your positions. Any spillage incident you cause can and will have an effect on your clearance. Accessing classified information outside the work environment could come up as part of an initial investigation or re-investigation as part of your clearance adjudication. It is therefore in your best interest to avoid anything that could constitute a spillage, or to stay away from anything that is questionable in nature such as WikiLeaks that could have a negative impact on your ability to obtain or maintain your clearance.

If you have any questions or concerns regard this matter, please see your immediate supervisor, or come see me or (b)(6) I appreciate your full and undivided attention in this matter.

/r

(b)(6)

(b)(6)

Director, MITSC HQMC
Administration and Resource Management Division
Office, Director of the Marine Corps Staff
Headquarters Marine Corps

(b)(6)

"~~FOR OFFICIAL USE ONLY.~~ Information contained within this document or its attachments may contain personnel information, disclosure of which is generally prohibited by the Privacy Act (5 U.S.C. 552a). Protected information included in this document or its attachments are in accordance with section (b)1 of the Act which permits disclosure to individuals within the Department of Defense (DoD) with an official need to know. Release of such protected information outside of the DoD is prohibited."

From:
To:
(b)(6)
Cc:
Subject: FW: PASS
Date: Wednesday, March 8, 2017 1:04:44 PM

Marines,

Please read, follow, and disperse between each other the below information from (b)(6)

R/S
(b)(6)
Pentagon, ARI Security Manager
Headquarters, United States Marine Corps (HQMC)
(b)(6)
"For true success, ask yourself these 4 questions: Why? Why not? Why not me? Why not now?
--James Allen

-----Original Message-----
From: (b)(6)
Sent: Wednesday, March 08, 2017 12:33 PM
To (b)(6)
(b)(6)
Subject: PASS

Pass the word to the Marines. DO NOT LOOK UP OR TRY TO LOOK UP MARINES UNITED or any associated wikileaks sites

R/s,
(b)(6)
ARI Operations Chief
(b)(6)

From: Nextgov Cybersecurity
To: (b)(6)
Subject: [EEMSG: Marketing][Non-DoD Source] House panels wants inventory of Kaspersky use; DOD"s smart device challenges; U.S. embassies vulnerable to digital snooping
Date: Tuesday, August 1, 2017 6:04:12 AM

Nextgov Cybersecurity

August 1, 2017

House Panel Wants Inventory of Agencies' Kaspersky Use // Joseph Marks

The Science, Space and Technology Committee is the latest to question how the government may be using the Russian anti-virus software.

DOD Needs to Lock Down Smart TVs to Prevent Surveillance, Watchdog Says // Jack Corrigan

The Defense Department needs to step security of connected devices, according to a recent report.

U.S. Embassies are Vulnerable to Digital Snooping, Watchdogs Find // Joseph Marks

Embassies' telecom supply chains often go through China and they aren't fixing vulnerabilities security officers point out.

A Fake Cyber Stat Lives On in Congress // Nextgov Staff

Some numbers are too convincing to go away.

Time to Choose a Password Manager // Caitlin Fairchild

Using a password manager is just one way to increase personal online security.

Senators OK Funding to Improve Their Own Cybersecurity // Joseph Marks

The funding bump would raise the upper chamber's cyber protections and train senators and staff in cyber hygiene.

Security Researcher Finds Mac Malware Spying on Home Computers

Technology

If youve heard the phrase there arent viruses for Macs, think again. A researcher with security firm Synack said at least 400 Macs ... Read more »

400,000 Italian Bank Customers Exposed in Breaches

Financial Services // Italy

UniBank, Italys largest bank, said the data of more than 400,000 customers was accessed twice during the last ten months, Reuters ... Read more »

Swedish Agency Skirts Its Own Security Rules, Exposes Data of Millions

Government (Foreign) // Sweden

The Swedish prime minister acknowledged a massive leak that exposed personal details about millions of Swedes, including anyone with a ... Read more »

Government Executive Media Group, 600 New Hampshire Avenue NW, Washington, DC 20037

From: GovExec PM update
To: (b)(6)
Subject: [Non-DoD Source] Consumer bureau chief steps down; DHS sniffing dog training in D.C.; How data is transforming government
Date: Wednesday, November 15, 2017 4:18:46 PM

Problems viewing? View as a web page

GovExec PM Update

November 15, 2017

Embattled Consumer Protection Bureau Chief Steps Down // Charles S. Clark

Cordray outlasted Republican calls for his head, but bureau's future is unclear.

Homeland Security Brings Explosive Detection Training to D.C.-Area Police Dogs // Ross Gianfortune

Program is critical in the fight against terrorism because state and local police are the first responders to any potential threat, official notes.

How Data-Driven Insight Is Transforming Government // John Kamensky

The use of analytics goes beyond just collecting and reporting evidence of program outcomes.

Play of the Day: WikiLeaks and the Trump Campaign // Ross Gianfortune

Maybe Donald Trump Jr. just thought he was looking something up on Wikipedia.

Syracuse Mayor Discusses How Tech and Data Intersect on Her City's Streets // Dave Nyczepir

As she prepares to leave office, Stephanie Miner looks back on an innovation-focused municipal agenda and where cities are going in the Trump era.

Pros and Cons of the New Digital Pills That Connect to Your Smartphone // Chase Purdy

This pill can even send data to your doctor.

From: Defense One Today
To: (b)(6)
Subject: [EEMSG: Marketing][Non-DoD Source] Chelsea Manning's Campaign Website is Based in Iceland. Why? / US General to Turkey: We're Not Pulling Back
Date: Monday, January 29, 2018 6:56:00 AM

Problems viewing? View as a web page

Defense One Today

January 29, 2018

Brought to you by Northrop Grumman

Chelsea Manning's Campaign Website is Based in Iceland. Why? / US General to Turkey: We're Not Pulling Back // Robinson Meyer

Experts warn that the world is now as dangerous as it was at the height of the Cold War. Many Americans already know it.

Chelsea Manning's Campaign Website is Based in Iceland. Why? // Patrick Tucker

For one thing, it's harder for U.S. law enforcement to search. That may matter to the Wikileaks contributor-turned-U.S. Senate candidate.

DHS Cyber Info Sharing Tool to Get a Reboot This Year // Joseph Marks

The goal is for organizations to use the tool to automatically block cyber threats.

How the Saudis Drag the US into Perpetual War in the Mideast // Danny Sjursen

With ISIS essentially gone from Syria, it's time to bug out, no matter what the Kingdom thinks.

US General to Turkey: We're Not Pulling Back // Kevin Baron

General Votel said the US supports its NATO ally's concerns but won't abandon the coalition of Syrian Democratic Forces fighting ISIS on the world's behalf.

Podcast: The War in Yemen and the Making of a Chaos State // Ben Watson

More than 1,000 days of fighting have turned Yemen into one of the most dangerous places on the planet. Aid workers, journalists, and experts explain little-appreciated realities about the war, and how — just maybe — to help turn things around.

Government Executive Media Group, 600 New Hampshire Avenue NW, Washington, DC 20037

From: (b)(6)
To:
Subject: [EEMSG: Marketing][Non-DoD Source] Keynote speaker announcement: GRC Summit 2018
Date: Wednesday, April 4, 2018 1:38:45 PM

Hi (b)(6)

I am excited to announce that **General Charles Frank Bolden** will be one of our keynote speakers at the Governance, Risk and Compliance Summit 2018. General Bolden is a retired Marine Corps Major General, former NASA administrator and astronaut.

In addition to General Bolden, our other keynote speakers include **Ashden Fein**, Associate - Covington & Burling LLP, who was the lead prosecutor in the famous Bradley Manning WikiLeaks trial, and **Gary Cokins**, CEO and founder of Analytics-Based Performance Management LLC.

There will be over 60 sessions for you to choose from at the GRC Summit this year. They are divided into six tracks, namely risk, audit & compliance, technology, deep-dive workshops, mSIG and the MetricStream app showcase. For more information on the agenda and the various tracks – www.grc-summit.com/us/2018/agenda.php

Some of the highlights include:

Case studies and expert talks:

- From risk management to performance: Upping the game for ERM
- EU GDPR compliance –What does audit need to know?
- Integrated GRC case study on risk management review by Salesforce.com
- Achieving sustainable business resilience: Learnings from a practitioner
- Risk analytics driving performance by Hancock Whitney Bank
- Beyond compliance- Driving value for your organization

Senior practitioner panel discussions:

- Measures to improve board level cybersecurity governance and oversight
- The role of internal audit in ensuring the effectiveness of risk and compliance programs
- Evolution of operational risk management- Adapting to regulatory changes and evolving risk frameworks
- Creating a robust strategy to align risk to performance

You can save $1,200 per attendee pass by using the special discount code **LPMS1399** and registering on https://www.grc-summit.com/us/2018/register.html. This offer is valid until the 30th of April, you can e-mail us at grc-summit@metricstream.com or call us +1-650-332-0342.

Book now to avoid missing out on this amazing deal! Looking forward to seeing you 3 - 6 June at the Marriott Waterfront, Baltimore MD

Best Regards,
Emaad Naseer
GRC Summit Team
+1-650-332-0342

From: Military.com
To: (b)(6)
Subject: [Non-DoD Source] Pentagon May Tap Military Pay, Pensions for Border Wall
Date: Tuesday, March 12, 2019 3:41:41 PM

Military.com

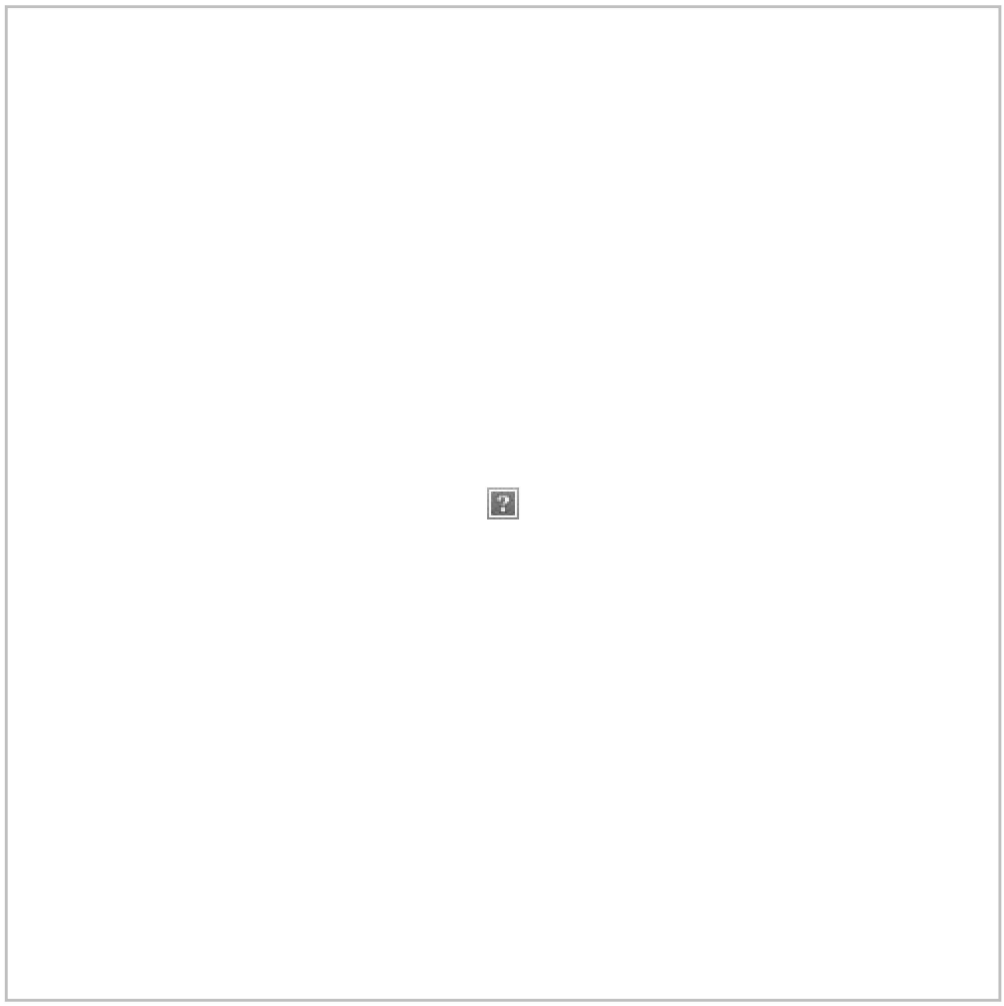
MARINES INSIDER

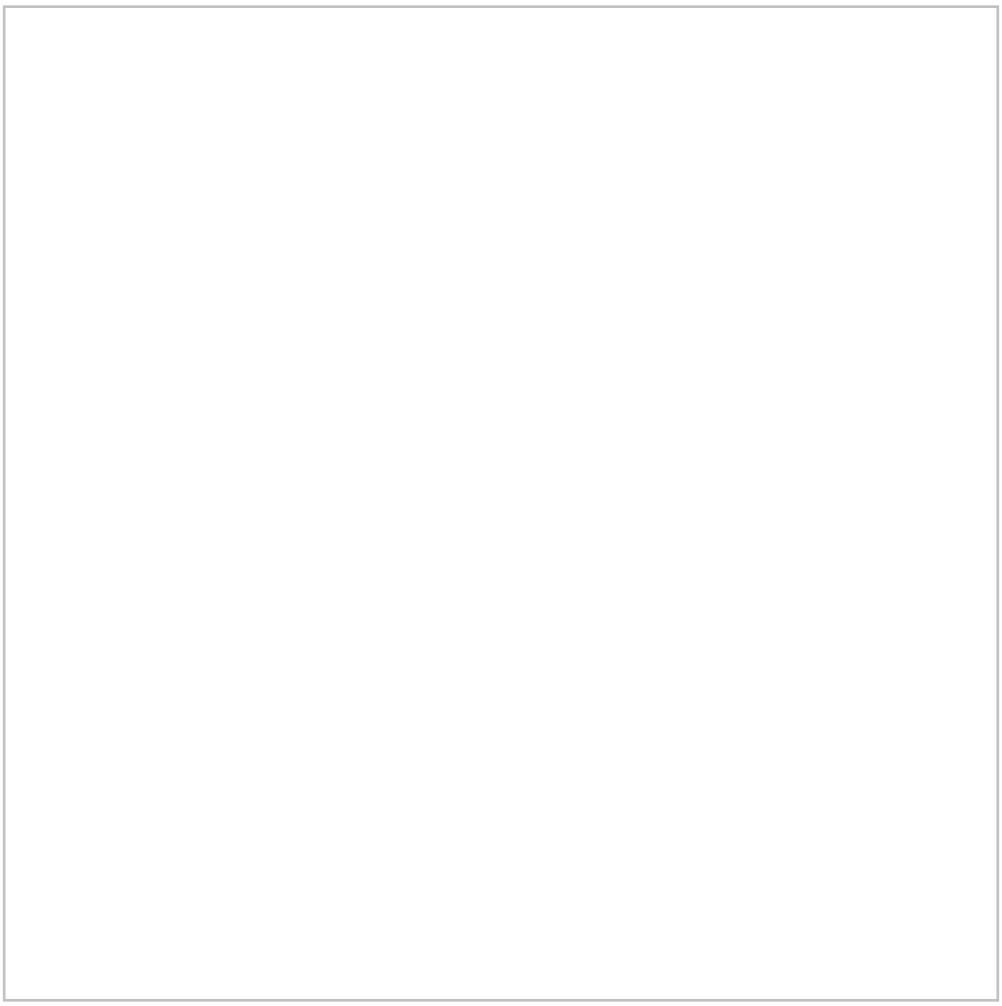
12 March 2019

Pentagon May Tap Military Pay, Pensions for Border Wall

Durbin says the funds are available because recruitment is down and an early military retirement program is underutilized.

Read More





Latest Military News

Lawmakers: End Afghanistan War, Give Every GWOT Vet a $2,500 Bonus

Will the VA Pay for Your Funeral? The Answer May Surprise You

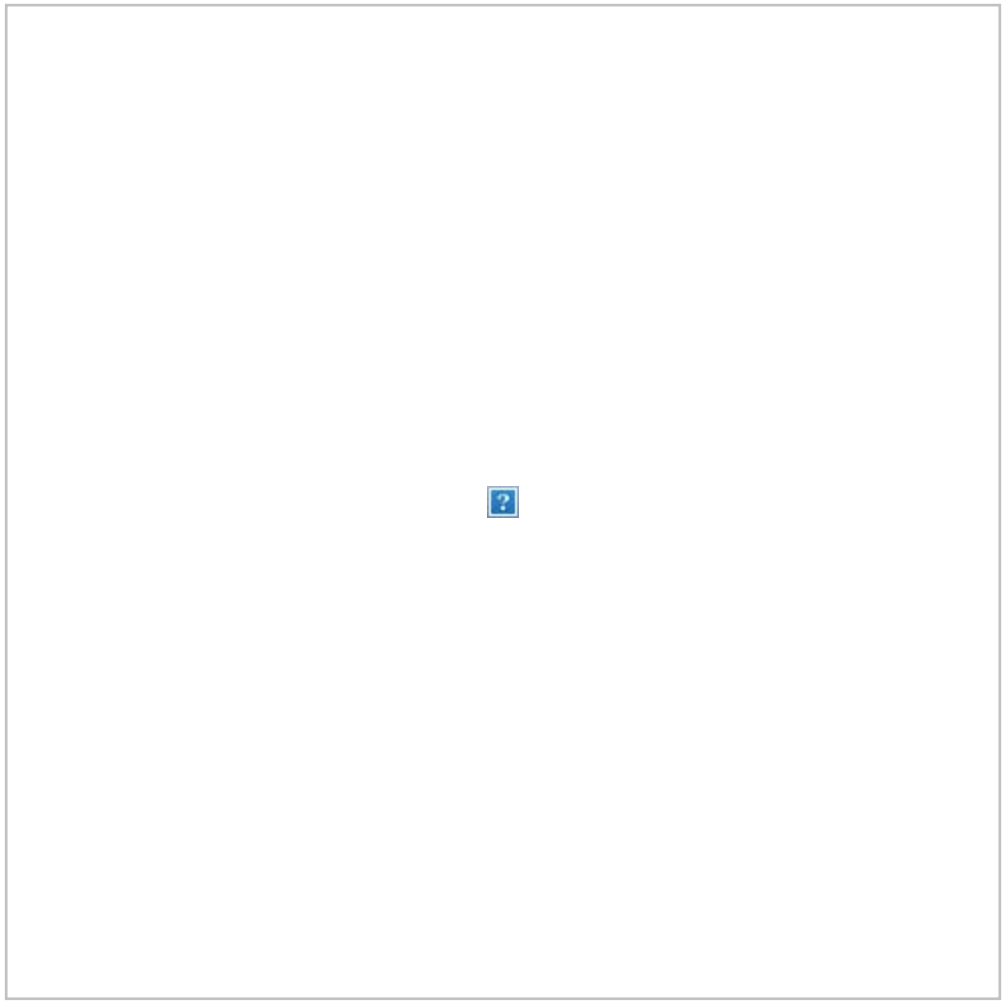
Tech Problems Delay Rollout of Expanded VA Caregiver Program

Quantico Case Raises Questions About How Marine Corps Handles Domestic Abuse

It’s Official: 2020 Budget Proposal Has Largest Troop Pay Raise in a Decade

Trump Signs Executive Order Creating Task Force to Stop Vet Suicide

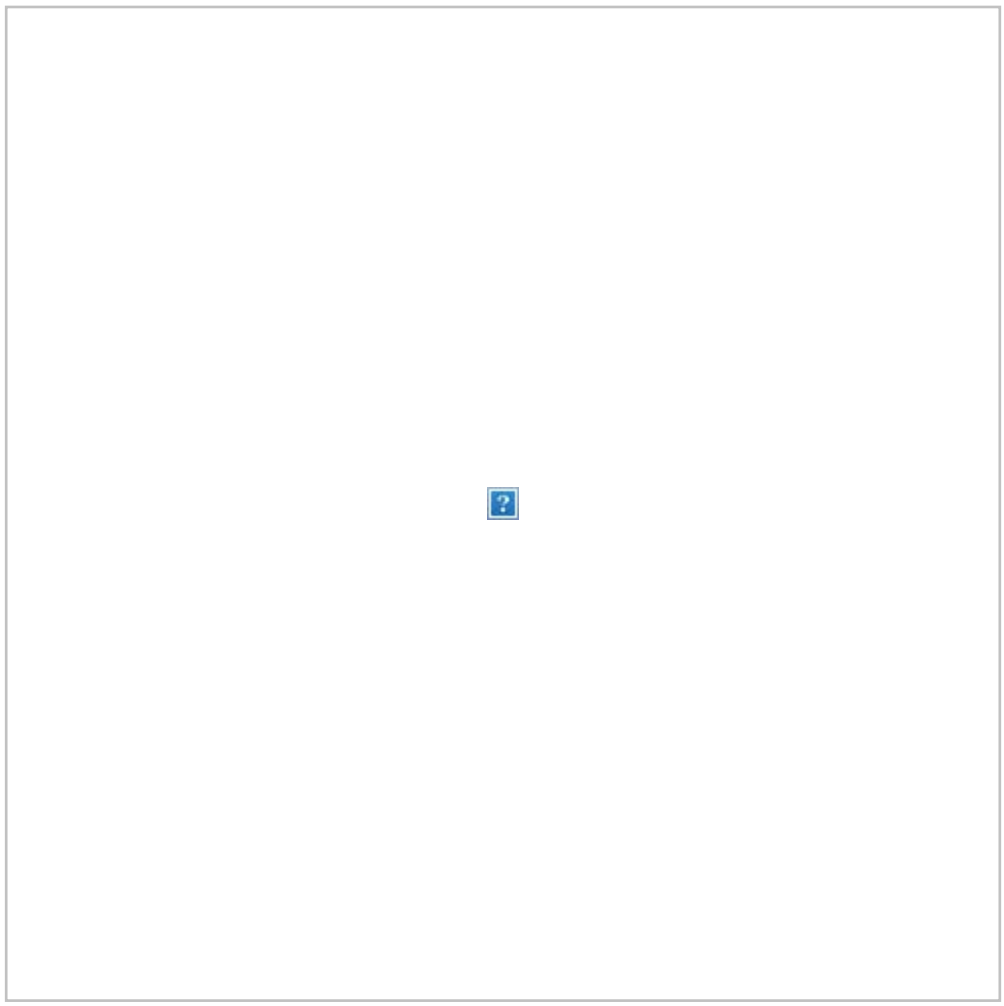
Air Force Gets First Upgraded 'Ghostrider' Gunship



Veterans Receive Golden 'Tickets' Canceling Their Medical Debt

Homeless Marine Veteran Charged in GoFundMe Scheme Pleads Guilty

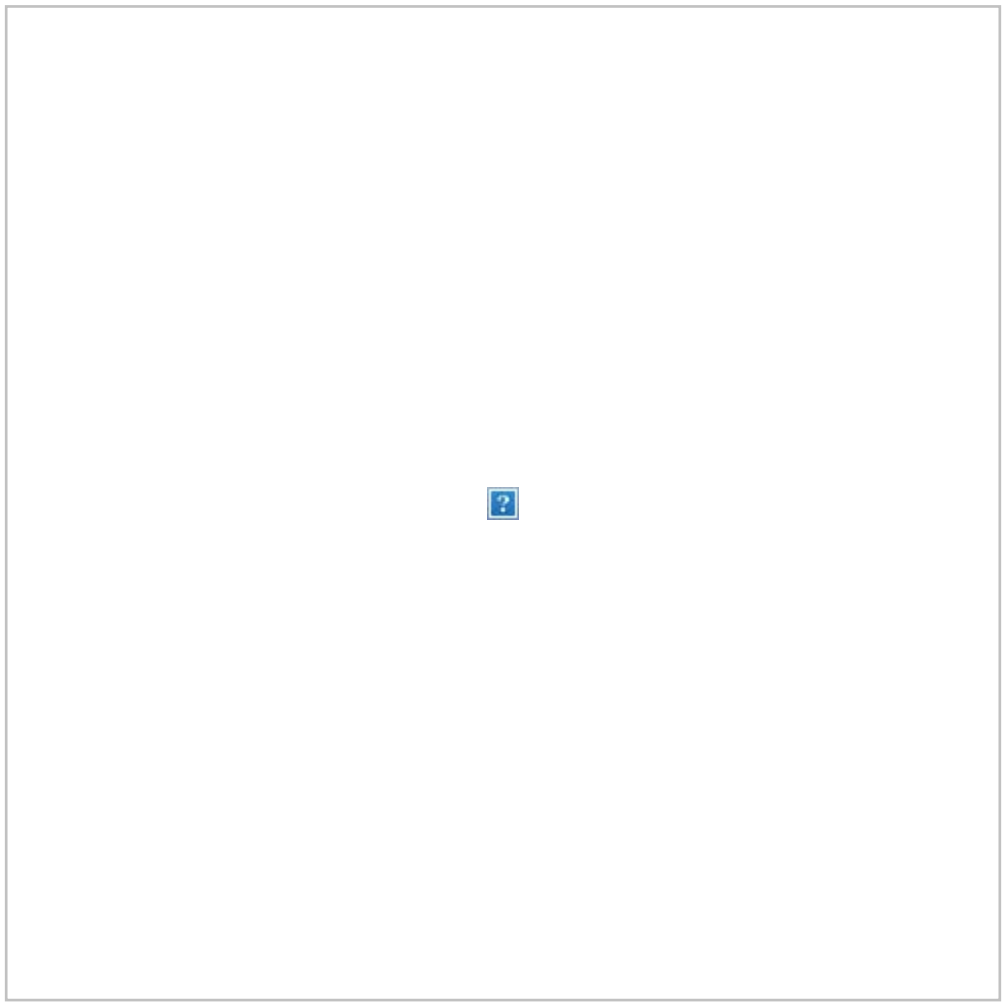
Two Marine Hornets Collide at Twentynine Palms; No Injuries Reported



This Coast Guard Pilot Braved a Hurricane and Made History in the Process

House Unanimously Passes Bill to Improve Burn Pit Registry

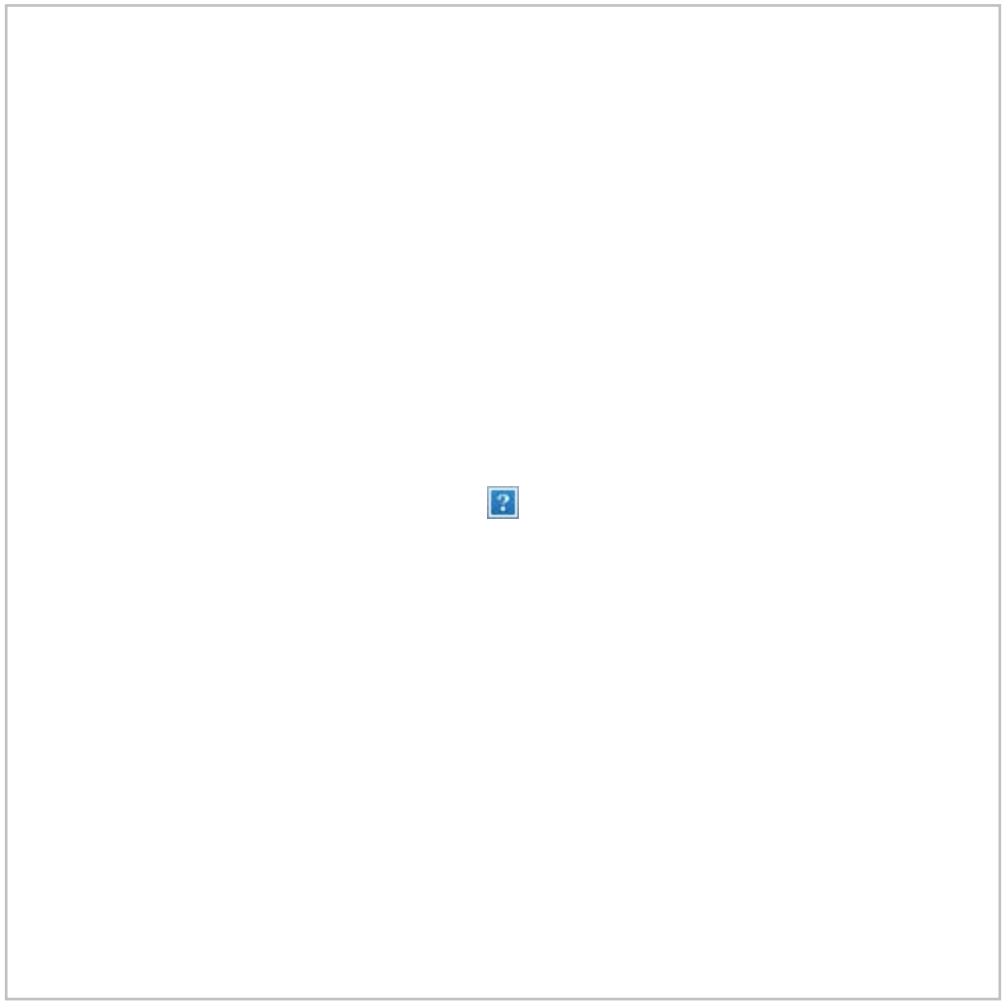
VA Waited 10 Months to Tell Vet He Had Cancer



Pentagon Debuts Draft Tenant Bill of Rights for Troops on Eve of Major Hearing

Proposed VA Budget Will Not Expand Private Care Funding, Officials Say

Check Out These 17 Awesome Photos of Military Working Dogs at War



VA Struggles to Curb Harassment of Female Veterans at Medical Centers

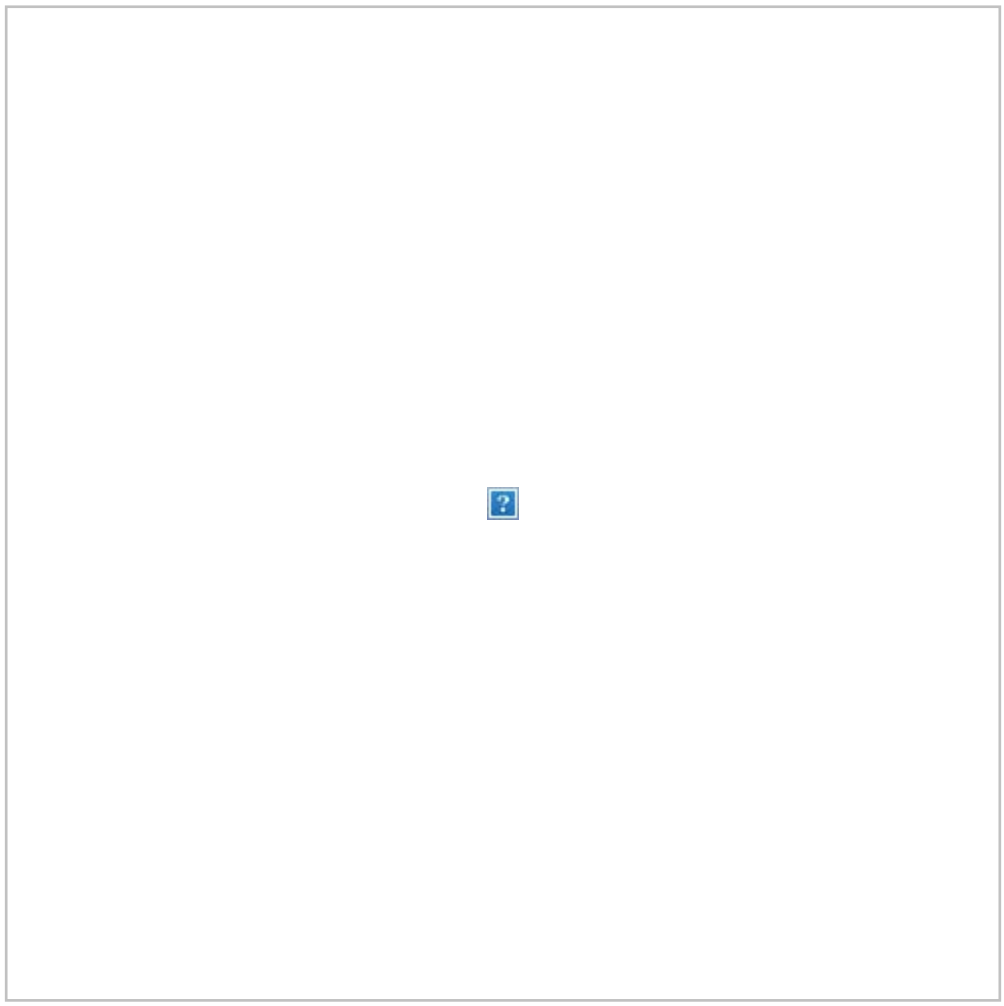
What Job Would Captain Marvel Have if She Were a Vet in Real Life?

Tricare Restricts Purchases of Deluxe Breast Pumps After $16 Million Overspend

Army IDs 2 Soldiers Killed in Kuwait Vehicle Collision

Chelsea Manning Jailed for Refusing to Testify on WikiLeaks

Among Veterans Organizations, Health Care, Suicide and Education Are Top Priorities



Videos of the Week

What a B-52 Bombing Run Looks Like

Su-27 Intercepts US RC-135 Spy Plane near Russian Border

Go Anywhere with the EZRaider Electric all Terrain Vehicle

Watch More Military.com Originals

Download our Military News App!

App Store

Google Play

You are subscribed to the Marine Insider.
Unsubscribe | Change Subscriber Options | Privacy Policy





Reach millions of people in the military community. Advertise with us

55 2nd Street, Suite 300, San Francisco, CA 94105

From: FCW Insider
To: (b)(6)
Subject: [EEMSG: Marketing][Non-DoD Source] IRS wants $2.7 billion to modernize IT | Navy looks to add cyber leadership
Date: Friday, April 12, 2019 7:20:24 AM

FCW Insider: April 12

The **IRS** is seeking **$2.7 billion** from Congress to modernize its legacy IT over the next six years. But some lawmakers are worried the tax agency is throwing good money after bad. Derek B. Johnson has the story.

Navy Secretary **Richard Spencer** says adding a new assistant secretary for cybersecurity and tightening contractors' security practices are top priorities for 2020. The pitch to Congress comes in the wake of a scathing internal report on the Navy's cyber vulnerabilities. Lauren C. Williams explains.

The **U.S. Air Force** is looking to attract and retain talent by providing paths to promotion through a new slate of disciplines, including intelligence, space and cybersecurity. Lauren reports on the new USAF career categories.

ACT-IAC named **David Wennergren** as its new CEO. The longtime federal IT executive will succeed **Kenneth Allen** to lead the industry-government organization. Anne Armstrong reports.

WikiLeaks founder **Julian Assange** was ejected from the Ecuadorian embassy in London where he'd spent almost seven years and arrested by British authorities on local charges and because of a U.S. indictment that claims he conspired to hack into a classified U.S. government system. What does the case mean for cybersecurity and for press freedom? Derek takes a look.

Quick Hits

*** The new Department of Homeland Security's C-suite is taking shape after the ouster of former Secretary **Kirstjen Nielsen** and former Acting Deputy Secretary **Claire Grady**. **David P. Pekoske**, administrator of the Transportation Security Administration, is taking over the duties of deputy secretary. Before his TSA post, Pekoske served as vice commandant of the U.S. Coast Guard.

*** The **Department of Defense** is looking for a contractor to perform administration, management support, security engineering, desktop support, communications and other duties on its 10-year, $10 billion enterprise-wide cloud acquisition. The request was posted on FedBizOpps just a day before it became publicly known that the **Joint Enterprise Defense Infrastructure** procurement had been winnowed down to two bidders -- **Amazon Web Services** and **Microsoft**.

*** **Russell Vought**, acting director of the Office of Management and Budget, reminded federal agency chiefs in an April 11 memorandum that the Office of Information and Regulatory Affairs at OMB is the hub of rulemaking under the Congressional Review Act. The memo reiterates some of the definitions and analyses to be used by agencies that loops in OIRA before agencies share rulemaking reports with Congress and the Government Accountability Office, as required under the Congressional Review Act.

More from FCW

IRS wants $2.7 billion over six years to modernize IT

The IRS chief detailed an ambitious plan to fix the agency's longstanding IT modernization problems over the next six years.

Navy looks to add cyber leadership

Navy Secretary Richard Spencer says adding a new assistant secretary for cybersecurity and tightening contractors' security practices are top

priorities for 2020.

Assange arrested, charged with hacking in 2010 Manning leaks

An attempt to crack a password that gave access to classified information is at the heart of criminal charges against WikiLeaks founder Julian Assange.

Cyber is among new USAF competitive career categories

The Air Force is trying to improve training and talent retention by adding seven new competitive career categories for officers that will include cyber, intelligence and space.

ACT-IAC names David Wennergren as its new CEO

The longtime federal IT executive will succeed Kenneth Allen to lead the industry-government organization.

JEDI cloud deal down to AWS and Microsoft

A Defense Department probe into conflict of interest relating to its $10 billion cloud buy didn't find anything to derail the solicitation. An award could be coming in mid-July.

Will DHS leadership upheaval affect CISA?

As the Department of Homeland Security scrambles following the abrupt departures of Secretary Kirstjen Nielsen and number of top officials, the newly formed Cybersecurity and Infrastructure Security Agency could get caught up in the chaos.

Advocacy group sues Education Department over blacklisted website

The advocacy group Public Citizen claims that the Education Department networks are blocking its website.

National Guard looks to industry for weekend cyber warriors

The National Guard wants to increase cybersecurity capacity by attracting exiting servicemembers and full-time private-sector professionals.

FCW
1105 Government Information Group
8251 Greensboro Drive, Suite 510
McLean, VA 22102
703-876-5100B

UNAUTHORIZED DISCLOSURE TRAINING

Date Signed: 10/5/2017
MARADMINS Number: 552/17

R 051809Z OCT 17
MARADMIN 552/17
MSGID/GENADMIN/CMC WASHINGTON DC PPO PS//
SUBJ/UNAUTHORIZED DISCLOSURE TRAINING//
REF/A/SECDEF MEMO DOD TRAINING ON UNAUTHORIZED DISCLOSURES DTD 19 SEP 2017/NOTAL//
REF/B/DOD 5200.01//
REF/C/DEPARTMENT OF DEFENSE DIRECTIVE 5230.09://
REF/D/SECNAV M-5510.36//
REF/E/MCO 5510.18B//
NARR/REF A MANDATES UNAUTHORIZED DISCLOSURE TRAINING FOR ALL DOD DEPARTMENTS AND AGENCIES IN OCTOBER 2017. REF B IS THE NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL. REF C IS THE DEPARTMENT OF DEFENSE DIRECTIVE ON CLEARANCE OF DOD INFORMATION FOR PUBLIC RELEASE. REF D IS THE DEPARTMENT OF THE NAVY INFORMATION SECURITY PROGRAM. REF E IS THE MARINE CORPS INFORMATION AND PERSONNEL SECURITY ORDER.//
POC (b)(6)
(b)(6)
GENTEXT/REMARKS/1. The spate of unauthorized disclosures of Classified Military Information (CMI) and Controlled Unclassified Information (CUI) has significantly weakened our governments ability to conduct business and protect the nation. The reasons and excuses for these occurrences are many and varied. They are also immaterial since it is illegal, immoral, and a violation of the oath we have taken to protect classified information as well as the oath we take to protect the Constitution of the United States against all enemies, foreign and domestic.
2. Accordingly, the Secretary of Defense has directed that every DOD department and agency dedicate one hour, during the month of October, to engage their organization in discussion of the importance of protecting this information from unauthorized

disclosure. Ref A pertains. This MARADMIN implements that direction.

2.A. All commands in the Marine Corps will conduct a one hour training session no later than the end of October 2017 on the topic of unauthorized disclosure. The following tools are available to assist in developing this training.

2.A.1 Video available for use: https:(slash)(slash) www.c-span.org/video/?432127-1/attorney-general-says-culture-leaking-must-stop&live

2.A.2 Center for Development of Security Excellence tool kit for training is available on its website (information security section): https:(slash)(slash)securityawareness.usalearning.gov/

3. As a reminder, Refs B, C, and D require commands to develop policies to ensure all information that will be released to the public undergo a security review prior to release. This includes speeches, information released by Family Readiness Officers, and information placed on public facing webpages. The next revision of Ref E will incorporate this requirement.

4. Point of contact is (b)(6)

(b)(6)

5. Release authorized by (b)(6) Deputy Director, Plans, Policies, and Operations (Security).//

NOTICE TO DOD EMPLOYEES AND CONTRACTORS
ON PROTECTING CLASSIFIED INFORMATION AND THE INTEGRITY OF UNCLASSIFIED GOVERNMENT INFORMATION TECHNOLOGY (IT) SYSTEMS

The recent disclosure of U.S. Government documents by WikiLeaks has caused damage to our national security. Each DoD employee and contractor is obligated to protect classified information and the integrity of government IT systems in accordance with applicable laws and DoD policies.

Unauthorized disclosures of classified documents (whether in print, on a blog, or on websites) do not alter the documents' classified status or automatically result in declassification of the documents. To the contrary, *classified information, whether or not already posted on public websites or disclosed to the media, remains classified, and must be treated as such by DoD employees and contractors, until it is declassified by an appropriate original classification authority*.

DoD employees and contractors are reminded of the following obligations with respect to protecting classified information and the integrity of unclassified government IT systems.

- DoD employees or contractors shall not access classified information unless they have:
    - received a favorable determination of eligibility for access by an appropriate authority,
    - signed an approved nondisclosure agreement,
    - demonstrated a need to know the information, and
    - received training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.
- DoD employees or contractors shall not remove classified information from official premises or disclose it without proper authorization.
- Except as authorized by DoD policy and procedures, DoD employees or contractors shall not, while accessing the web on unclassified government systems (including BlackBerries or other smartphones), access or download documents that are marked classified (including classified documents publicly available on WikiLeaks.org and other websites), as doing so risks putting classified information on unclassified IT systems.
    - This requirement applies to accessing or downloading that occurs using government computers or employees' or contractors' personally owned computers that access unclassified government systems, either through remote Outlook access or other remote access capabilities that enable connection to these government systems.

This requirement does not restrict employee or contractor access to unclassified, publicly available news reports (and other unclassified material) that may in turn discuss classified material, as distinguished from access to the underlying classified documents available on public websites or otherwise in the public domain.

- DoD employees or contractors shall refer all public queries on this matter to their servicing Public Affairs office; they shall neither confirm nor deny the presence of classified information in articles or websites in the public domain.

- DoD employees or contractors shall refer Congressional queries pertaining to the presence of classified information in articles or websites in the public domain to their servicing Congressional Affairs office.

- DoD employees and contractors who believe they have inadvertently accessed or downloaded classified information from a public website via an unclassified government IT system, or without prior authorization, shall contact their information assurance manager (IAM) or information assurance office (IAO) for assistance. *Note: In the case of classified documents inadvertently accessed or downloaded from the WikiLeaks website or other websites posting WikiLeaks-related classified documents, the IAM will document each occurrence and delete the affected file(s) by holding down the SHIFT key while pressing the DELETE key for Windows-based systems. No incident report or further sanitization of government IT systems is required. This guidance pertains only to the accessing or downloading of the classified documents described above because of the extent of the compromise and the prohibitive cost of standard sanitization procedures. All other classified spillages must be handled in accordance with existing regulations.*

Thank you for your cooperation and vigilance in implementing these responsibilities.

FW SAFEGUARDING CLASSIFIED NATIONAL SECURITY INFORMATION

-----Original Message-----
From: (b)(6)
Sent: Friday, August 8, 2014 12:30 PM
To: M_HQMC_IL <M_HQMC_IL@usmc.mil>
Subject: SAFEGUARDING CLASSIFIED NATIONAL SECURITY INFORMATION

REQUEST WIDEST DISSEMINATION

Ladies and Gentlemen,

1. As a reminder, classified information, whether or not already posted on public websites or disclosed to the media, remains classified and must be treated as such until it is declassified by an appropriate U.S. Government authority.

2. It is the responsibility of every DoD employee and contractor to protect classified information and to follow established procedures for accessing classified information only through authorized means. Security Coordinators must maintain a vigilant climate within their staff agencies/activities that underscores the critical importance of safeguarding classified material against compromise.

3. The attachment serves as a notice to all employees with access to classified material, of the responsibilities associated with the protection of classified information. Strict adherence to policy is expected of all employees, to include prompt reporting when violations of these policies occur.

4. If you have any questions please contact your Security Coordinator or Command Security Manager. For I&L, (b)(6) can be reached at (b)(6) and for MCICOM, (b)(6) can be reached at

V/r

(b)(6)
Security Manager
Headquarters U.S. Marine Corps
3000 Marine Corps Pentagon Rm (b)(6)
Washington, DC 20350-3000

(b)(6)

~~FOR OFFICIAL USE ONLY~~

THIS TRANSMISSION CONTAINS PERSONAL OR PRIVILEGED INFORMATION AND SHOULD BE TREATED AS "~~FOR OFFICIAL USE ONLY".~~ CONTENTS THEREOF SHALL NOT BE

FW SAFEGUARDING CLASSIFIED NATIONAL SECURITY INFORMATION DISCLOSED, DISCUSSED, OR SHARED WITH INDIVIDUALS UNLESS THEY HAVE A DIRECT NEED TO KNOW IN THE PERFORMANCE OF THEIR OFFICIAL DUTIES. ANY UNAUTHORIZED DISCLOSURE OF THE INFORMATION MAY RESULT IN CIVIL AND CRIMINAL PENALTIES UNDER THE PRIVACY ACT OF 1974. IF YOU ARE NOT THE INTENDED RECIPIENT OR BELIEVE YOU HAVE RECEIVED THIS IN ERROR, DO NOT COPY, DISSEMINATE OR OTHERWISE USE THE INFORMATION AND CONTACT THE CREATOR/OWNER OF THIS TRANSMISSION OR YOUR PRIVACY ACT OFFICER DOD DIRECTIVE 5400.11, DEPARTMENT OF DEFENSE PRIVACY PROGRAM," AND 32 CFR 701.F, AND 701.G

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

November 28, 2010

M-11-06

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Jacob J. Lew (b)(6)
Director

SUBJECT: WikiLeaks - Mishandling of Classified Information

Our national defense requires that sensitive information be maintained in confidence to protect our citizens, our democratic institutions, and our homeland. Protecting information critical to our nation's security is the responsibility of each individual who is granted access to classified information. Any unauthorized disclosure of classified information is a violation of our law and compromises our national security.

The recent irresponsible disclosure by WikiLeaks has resulted in significant damage to our national security. Any failure by agencies to safeguard classified information pursuant to relevant laws, including but not limited to Executive Order 13526, *Classified National Security Information* (December 29, 2009), is unacceptable and will not be tolerated.

Please note the following immediate instructions:

- Each department or agency that handles classified information shall establish a security assessment team consisting of counterintelligence, security, and information assurance experts to review the agency's implementation of procedures for safeguarding classified information against improper disclosures. Such review should include (without limitation) evaluation of the agency's configuration of classified government systems to ensure that users do not have broader access than is necessary to do their jobs effectively, as well as implementation of restrictions on usage of, and removable media capabilities from, classified government computer networks.

- The Office of Management and Budget, the Information Security Oversight Office, and the Office of the Director of National Intelligence will stand up processes to evaluate, and to assist agencies in their review of, security practices with respect to the protection of classified information.

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release October 7, 2011

EXECUTIVE ORDER

- - - - - - -

STRUCTURAL REFORMS TO IMPROVE THE SECURITY OF CLASSIFIED NETWORKS AND THE RESPONSIBLE SHARING AND SAFEGUARDING OF CLASSIFIED INFORMATION

By the authority vested in me as President by the Constitution and the laws of the United States of America and in order to ensure the responsible sharing and safeguarding of classified national security information (classified information) on computer networks, it is hereby ordered as follows:

Section 1. Policy. Our Nation's security requires classified information to be shared immediately with authorized users around the world but also requires sophisticated and vigilant means to ensure it is shared securely. Computer networks have individual and common vulnerabilities that require coordinated decisions on risk management.

This order directs structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties. Agencies bear the primary responsibility for meeting these twin goals. These structural reforms will ensure coordinated interagency development and reliable implementation of policies and minimum standards regarding information security, personnel security, and systems security; address both internal and external security threats and vulnerabilities; and provide policies and minimum standards for sharing classified information both within and outside the Federal Government. These policies and minimum standards will address all agencies that operate or access classified computer networks, all users of classified computer networks (including contractors and others who operate or access classified computer networks controlled by the Federal Government), and all classified information on those networks.

Sec. 2. General Responsibilities of Agencies.

Sec. 2.1. The heads of agencies that operate or access classified computer networks shall have responsibility for appropriately sharing and safeguarding classified information on computer networks. As part of this responsibility, they shall:

(a) designate a senior official to be charged with overseeing classified information sharing and safeguarding efforts for the agency;

(b) implement an insider threat detection and prevention program consistent with guidance and standards developed by the Insider Threat Task Force established in section 6 of this order;

(c) perform self-assessments of compliance with policies and standards issued pursuant to sections 3.3, 5.2, and 6.3 of this order, as well as other applicable policies and standards, the results of which shall be reported annually to the Senior Information Sharing and Safeguarding Steering Committee established in section 3 of this order;

(d) provide information and access, as warranted and consistent with law and section 7(d) of this order, to enable independent assessments by the Executive Agent for Safeguarding Classified Information on Computer Networks and the Insider Threat Task Force of compliance with relevant established policies and standards; and

(e) detail or assign staff as appropriate and necessary to the Classified Information Sharing and Safeguarding Office and the Insider Threat Task Force on an ongoing basis.

Sec. 3. Senior Information Sharing and Safeguarding Steering Committee.

Sec. 3.1. There is established a Senior Information Sharing and Safeguarding Steering Committee (Steering Committee) to exercise overall responsibility and ensure senior-level accountability for the coordinated interagency development and implementation of policies and standards regarding the sharing and safeguarding of classified information on computer networks.

Sec. 3.2. The Steering Committee shall be co-chaired by senior representatives of the Office of Management and Budget and the National Security Staff. Members of the committee shall be officers of the United States as designated by the heads of the Departments of State, Defense, Justice, Energy, and Homeland Security, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the Information Security Oversight Office within the National Archives and Records Administration (ISOO), as well as such additional agencies as the co-chairs of the Steering Committee may designate.

Sec. 3.3. The responsibilities of the Steering Committee shall include:

(a) establishing Government-wide classified information sharing and safeguarding goals and annually reviewing executive branch successes and shortcomings in achieving those goals;

(b) preparing within 90 days of the date of this order and at least annually thereafter, a report for the President assessing the executive branch's successes and shortcomings in sharing and safeguarding classified information on computer networks and discussing potential future vulnerabilities;

(c) developing program and budget recommendations to achieve Government-wide classified information sharing and safeguarding goals;

(d) coordinating the interagency development and implementation of priorities, policies, and standards for sharing and safeguarding classified information on computer networks;

(e) recommending overarching policies, when appropriate, for promulgation by the Office of Management and Budget or the ISOO;

(f) coordinating efforts by agencies, the Executive Agent, and the Task Force to assess compliance with established policies and standards and recommending corrective actions needed to ensure compliance;

(g) providing overall mission guidance for the Program Manager-Information Sharing Environment (PM-ISE) with respect to the functions to be performed by the Classified Information Sharing and Safeguarding Office established in section 4 of this order; and

(h) referring policy and compliance issues that cannot be resolved by the Steering Committee to the Deputies Committee of the National Security Council in accordance with Presidential Policy Directive/PPD-1 of February 13, 2009 (Organization of the National Security Council System).

Sec. 4. Classified Information Sharing and Safeguarding Office.

Sec. 4.1. There shall be established a Classified Information Sharing and Safeguarding Office (CISSO) within and subordinate to the office of the PM-ISE to provide expert, full-time, sustained focus on responsible sharing and safeguarding of classified information on computer networks. Staff of the CISSO shall include detailees, as needed and appropriate, from agencies represented on the Steering Committee.

Sec. 4.2. The responsibilities of CISSO shall include:

(a) providing staff support for the Steering Committee;

(b) advising the Executive Agent for Safeguarding Classified Information on Computer Networks and the Insider Threat Task Force on the development of an effective program to monitor compliance with established policies and standards needed to achieve classified information sharing and safeguarding goals; and

(c) consulting with the Departments of State, Defense, and Homeland Security, the ISOO, the Office of the Director of National Intelligence, and others, as appropriate, to ensure consistency with policies and standards under Executive Order 13526 of December 29, 2009, Executive Order 12829 of January 6, 1993, as amended, Executive Order 13549 of August 18, 2010, and Executive Order 13556 of November 4, 2010.

Sec. 5. Executive Agent for Safeguarding Classified Information on Computer Networks.

Sec. 5.1. The Secretary of Defense and the Director, National Security Agency, shall jointly act as the Executive Agent for Safeguarding Classified Information on Computer Networks (the "Executive Agent"), exercising the existing authorities of the Executive Agent and National Manager for national security systems, respectively, under National Security Directive/NSD-42 of July 5, 1990, as supplemented by and subject to this order.

Sec. 5.2. The Executive Agent's responsibilities, in addition to those specified by NSD-42, shall include the following:

(a) developing effective technical safeguarding policies and standards in coordination with the Committee on National Security Systems (CNSS), as re-designated by Executive Orders 13286 of February 28, 2003, and 13231 of October 16, 2001, that address the safeguarding of classified information within national security systems, as well as the safeguarding of national security systems themselves;

(b) referring to the Steering Committee for resolution any unresolved issues delaying the Executive Agent's timely development and issuance of technical policies and standards;

(c) reporting at least annually to the Steering Committee on the work of CNSS, including recommendations for any changes needed to improve the timeliness and effectiveness of that work; and

(d) conducting independent assessments of agency compliance with established safeguarding policies and standards, and reporting the results of such assessments to the Steering Committee.

Sec. 6. Insider Threat Task Force.

Sec. 6.1. There is established an interagency Insider Threat Task Force that shall develop a Government-wide program (insider threat program) for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels, as well as the distinct needs, missions, and systems of individual agencies. This program shall include development of policies, objectives, and priorities for establishing and integrating security, counterintelligence, user audits and monitoring, and other safeguarding capabilities and practices within agencies.

Sec. 6.2. The Task Force shall be co-chaired by the Attorney General and the Director of National Intelligence, or their designees. Membership on the Task Force shall be composed of officers of the United States from, and designated by the heads of, the Departments of State, Defense, Justice, Energy, and Homeland Security, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the ISOO, as well as such additional agencies as the co-chairs of the Task Force may designate. It shall be staffed by personnel from the Federal Bureau of Investigation and the Office of the National Counterintelligence Executive (ONCIX), and other agencies, as determined by the co-chairs for their respective agencies and to the extent permitted by law. Such personnel must be officers or full-time or permanent part-time employees of the United States. To the extent permitted by law, ONCIX shall provide an appropriate work site and administrative support for the Task Force.

Sec. 6.3. The Task Force's responsibilities shall include the following:

(a) developing, in coordination with the Executive Agent, a Government-wide policy for the deterrence, detection, and mitigation of insider threats, which shall be submitted to the Steering Committee for appropriate review;

(b) in coordination with appropriate agencies, developing minimum standards and guidance for implementation of the insider threat program's Government-wide policy and, within 1 year of the date of this order, issuing those minimum standards and guidance, which shall be binding on the executive branch;

(c) if sufficient appropriations or authorizations are obtained, continuing in coordination with appropriate agencies after 1 year from the date of this order to add to or modify those minimum standards and guidance, as appropriate;

(d) if sufficient appropriations or authorizations are not obtained, recommending for promulgation by the Office of Management and Budget or the ISOO any additional or modified minimum standards and guidance developed more than 1 year after the date of this order;

(e) referring to the Steering Committee for resolution any unresolved issues delaying the timely development and issuance of minimum standards;

(f) conducting, in accordance with procedures to be developed by the Task Force, independent assessments of the adequacy of agency programs to implement established policies and minimum standards, and reporting the results of such assessments to the Steering Committee;

(g) providing assistance to agencies, as requested, including through the dissemination of best practices; and

(h) providing analysis of new and continuing insider threat challenges facing the United States Government.

Sec. 7. General Provisions. (a) For the purposes of this order, the word "agencies" shall have the meaning set forth in section 6.1(b) of Executive Order 13526 of December 29, 2009.

(b) Nothing in this order shall be construed to change the requirements of Executive Orders 12333 of December 4, 1981, 12829 of January 6, 1993, 12968 of August 2, 1995, 13388 of October 25, 2005, 13467 of June 30, 2008, 13526 of December 29, 2009, 13549 of August 18, 2010, and their successor orders and directives.

(c) Nothing in this order shall be construed to supersede or change the authorities of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended; the Secretary of Defense under Executive Order 12829, as amended; the Secretary of Homeland Security under Executive Order 13549; the Secretary of State under title 22, United States Code, and the Omnibus Diplomatic Security and Antiterrorism Act of 1986; the Director of ISOO under Executive Orders 13526 and 12829, as amended; the PM-ISE under Executive Order 13388 or the Intelligence Reform and Terrorism Prevention Act of 2004, as amended; the Director, Central Intelligence Agency under NSD-42 and Executive Order 13286, as amended; the National Counterintelligence

Executive, under the Counterintelligence Enhancement Act of 2002; or the Director of National Intelligence under the National Security Act of 1947, as amended, the Intelligence Reform and Terrorism Prevention Act of 2004, as amended, NSD-42, and Executive Orders 12333, as amended, 12968, as amended, 13286, as amended, 13467, and 13526.

(d) Nothing in this order shall authorize the Steering Committee, CISSO, CNSS, or the Task Force to examine the facilities or systems of other agencies, without advance consultation with the head of such agency, nor to collect information for any purpose not provided herein.

(e) The entities created and the activities directed by this order shall not seek to deter, detect, or mitigate disclosures of information by Government employees or contractors that are lawful under and protected by the Intelligence Community Whistleblower Protection Act of 1998, Whistleblower Protection Act of 1989, Inspector General Act of 1978, or similar statutes, regulations, or policies.

(f) With respect to the Intelligence Community, the Director of National Intelligence, after consultation with the heads of affected agencies, may issue such policy directives and guidance as the Director of National Intelligence deems necessary to implement this order.

(g) Nothing in this order shall be construed to impair or otherwise affect:

(1) the authority granted by law to an agency, or the head thereof; or

(2) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(h) This order shall be implemented consistent with applicable law and appropriate protections for privacy and civil liberties, and subject to the availability of appropriations.

(i) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA

THE WHITE HOUSE,
October 7, 2011.

# # #

Leaked Reports Detail Iran's Aid for Iraqi Militias

http://www.nytimes.com
October 22, 2010
By MICHAEL R. GORDON and ANDREW W. LEHREN

On Dec. 22, 2006, American military officials in Baghdad issued a secret warning: The Shiite militia commander who had orchestrated the kidnapping of officials from Iraq's Ministry of Higher Education was now hatching plans to take American soldiers hostage.
What made the warning especially worrying were intelligence reports saying that the Iraqi militant, Azhar al-Dulaimi, had been trained by the Middle East's masters of the dark arts of paramilitary operations: the Islamic Revolutionary Guards Corps in Iran and Hezbollah, its Lebanese ally.

"Dulaymi reportedly obtained his training from Hizballah operatives near Qum, Iran, who were under the supervision of Iranian Islamic Revolutionary Guard Corps Quds Force (IRGC-QF) officers in July 2006," the report noted, using alternative spellings of the principals involved.

Five months later, Mr. Dulaimi was tracked down and killed in an American raid in the sprawling Shiite enclave of Sadr City in Baghdad — but not before four American soldiers had been abducted from an Iraqi headquarters in Karbala and executed in an operation that American military officials say literally bore Mr. Dulaimi's fingerprints.

Scores of documents made public by WikiLeaks, which has disclosed classified information about the wars in Iraq and Afghanistan, provide a ground-level look — at least as seen by American units in the field and the United States' military intelligence — at the shadow war between the United States and Iraqi militias backed by Iran's Revolutionary Guards.

During the administration of President George W. Bush, critics charged that the White House had exaggerated Iran's role to deflect criticism of its handling of the war and build support for a tough policy toward Iran, including the possibility of military action.

But the field reports disclosed by WikiLeaks, which were never intended to be made public, underscore the seriousness with which Iran's role has been seen by the American military. The political struggle between the United States and Iran to influence events in Iraq still continues as Prime Minister Nuri Kamal al-Maliki has sought to assemble a coalition — that would include the anti-American cleric Moktada al-Sadr — that will allow him to remain in power. But much of the American's military concern has revolved around Iran's role in arming and assisting Shiite militias.

Citing the testimony of detainees, a captured militant's diary and numerous uncovered weapons caches, among other intelligence, the field reports recount Iran's role in providing Iraqi militia

fighters with rockets, magnetic bombs that can be attached to the underside of cars, “explosively formed penetrators,” or E.F.P.’s, which are the most lethal type of roadside bomb in Iraq, and other weapons. Those include powerful .50-caliber rifles and the Misagh-1, an Iranian replica of a portable Chinese surface-to-air missile, which, according to the reports, was fired at American helicopters and downed one in east Baghdad in July 2007.

Iraqi militants went to Iran to be trained as snipers and in the use of explosives, the field reports assert, and Iran’s Quds Force collaborated with Iraqi extremists to encourage the assassination of Iraqi officials.

The reports make it clear that the lethal contest between Iranian-backed militias and American forces continued after President Obama sought to open a diplomatic dialogue with Iran’s leaders and reaffirmed the agreement between the United States and Iraq to withdraw American troops from Iraq by the end of 2011.

A Revolutionary Force

Established by Ayatollah Ruhollah Khomeini after the 1979 Iranian revolution, the Islamic Revolutionary Guards Corps has expanded its influence at home under President Mahmoud Ahmadinejad, a former member of the corps, and it plays an important role in Iran’s economy, politics and internal security. The corps’s Quds Force, under the command of Brig. Gen. Qassem Soleimani, has responsibility for foreign operations and has often sought to work though surrogates, like Hezbollah.

While the American government has long believed that the Quds Force has been providing lethal assistance and training to Shiite militants in Iraq, the field reports provide new details about Iran’s support for Iraqi militias and the American military’s operations to counter them.

The reports are written entirely from the perspective of the American-led coalition. No similar Iraqi or Iranian reports have been made available. Nor do the American reports include the more comprehensive assessments that are typically prepared by American intelligence agencies after incidents in the field.

While some of the raw information cannot be verified, it is nonetheless broadly consistent with other classified American intelligence and public accounts by American military officials. As seen by current and former American officials, the Quds Force has two main objectives: to weaken and shape Iraq’s nascent government and to diminish the United States’ role and influence in Iraq.

For people like General Soleimani, “who went through all eight years of the Iran-Iraq war, this is certainly about poking a stick at us, but it is also about achieving strategic advantage in Iraq,” Ryan C. Crocker, the American ambassador in Iraq from 2007 until early 2009, said in an interview.

“I think the Iranians understand that they are not going to dominate Iraq,” Mr. Crocker added, “ but I think they are going to do their level best to weaken it — to have a weak central government that is constantly off balance, that is going to have to be beseeching Iran to stop doing bad things without having the capability to compel them to stop doing bad things. And that is an Iraq that will never again threaten Iran.”

Politics and Militias

According to the reports, Iran’s role has been political as well as military. A Nov. 27, 2005, report, issued before Iraq’s December 2005 parliamentary elections, cautioned that Iranian-backed militia members in the Iraqi government were gaining power and giving Iran influence over Iraqi politics.

“Iran is gaining control of Iraq at many levels of the Iraqi government,” the report warned.

The reports also recount an array of border incidents, including a Sept. 7, 2006, episode in which an Iranian soldier who aimed a rocket-propelled grenade launcher at an American platoon trying to leave the border area was shot and killed by an American soldier with a .50-caliber machine gun. The members of the American platoon, who had gone to the border area with Iraqi troops to look for “infiltration routes” used to smuggle bombs and other weapons into Iraq, were concerned that Iranian border forces were trying to surround and detain them. After this incident, the platoon returned to its base in Iraq under fire from the Iranians even when the American soldiers were “well inside Iraqi territory,” a report noted.

But the reports assert that Iran’s Quds Force and intelligence service has turned to many violent and shadowy tactics as well.

The reports contain numerous references to Iranian agents, but the documents generally describe a pattern in which the Quds Force has sought to maintain a low profile in Iraq by arranging for fighters from Hezbollah in Lebanon to train Iraqi militants in Iran or by giving guidance to Iraqi militias who do the fighting with Iranian financing and weapons.

The reports suggest that Iranian-sponsored assassinations of Iraqi officials became a serious worry.

A case in point is a report that was issued on March 27, 2007. Iranian intelligence agents within the Badr Corps and Jaish al-Mahdi, two Shiite militias, “have recently been influencing attacks on ministry officials in Iraq,” the report said.

According to the March report, officials at the Ministry of Industry were high on the target list. “The desired effect of these attacks is not to simply kill the Ministry of Industry Officials,” the report noted, but also “to show the world, and especially the Arab world, that the Baghdad

Security Plan has failed to bring stability," referring to the troop increase that Gen. David H. Petraeus was overseeing to reduce violence in Iraq.

News reports in early 2007 indicated that a consultant to the ministry and his daughter were shot and killed on the way to his office. The March report does not mention the attack, but it asserts that one gunman was carrying out a systematic assassination campaign, which included killing three bodyguards and plotting to attack ministry officials while wearing a stolen Iraqi Army uniform.

The provision of Iranian rockets, mortars and bombs to Shiite militants has also been a major concern. A Nov. 22, 2005, report recounted an effort by the Iraqi border police to stop the smuggling of weapons from Iran, which "recovered a quantity of bomb-making equipment, including explosively formed projectiles," which are capable of blasting a metal projectile through the door of an armored Humvee.

A Shiite militant from the Jaish al-Mahdi militia, also known as the Mahdi Army, was planning to carry out a mortar attack on the Green Zone in Baghdad, using rockets and mortar shells shipped by the Quds Force, according to a report on Dec. 1, 2006. On Nov. 28, the report noted, the Mahdi Army commander, Ali al-Sa'idi, "met Iranian officials reported to be IRGC officers at the border to pick up three shipments of rockets."

A Dec. 27, 2008, report noted one instance when American soldiers from the 82nd Airborne Division captured several suspected members of the Jaish al-Mahdi militia and seized a weapons cache, which also included several diaries, including one that explained "why detainee joined JAM and how they traffic materials from Iran."

The attacks continued during Mr. Obama's first year in office, with no indication in the reports that the new administration's policies led the Quds Force to end its support for Iraqi militants. The pending American troop withdrawals, the reports asserted, may even have encouraged some militant attacks.

A June 25, 2009, report about an especially bloody E.F.P. attack that wounded 10 American soldiers noted that the militants used tactics "being employed by trained violent extremist members that have returned from Iran." The purpose of the attack, the report speculated, was to increase American casualties so militants could claim that they had "fought the occupiers and forced them to withdraw."

An intelligence analysis of a Dec. 31, 2009, attack on the Green Zone using 107-millimeter rockets concluded that it was carried out by the Baghdad branch of Kataib Hezbollah, a militant Shiite group that American intelligence has long believed is supported by Iran. According to the December report, a technical expert from Kataib Hezbollah met before the attack with a "weapons facilitator" who "reportedly traveled to Iran, possibility to facilitate the attacks on 31 Dec."

That same month, American Special Operations forces and a specially trained Iraqi police unit mounted a raid that snared an Iraqi militant near Basra who had been trained in Iran. A Dec. 19, 2009, report stated that the detainee was involved in smuggling “sticky bombs”— explosives that are attached magnetically to the underside of vehicles — into Iraq and was “suspected of collecting information on CF [coalition forces] and passing them to Iranian intelligence agents.”

A Bold Operation

One of the most striking episodes detailed in the trove of documents made public by WikiLeaks describes a plot to kidnap American soldiers from their Humvees. According to the Dec. 22, 2006, report, a militia commander, Hasan Salim, devised a plan to capture American soldiers in Baghdad and hold them hostage in Sadr City to deter American raids there.

To carry out the plan, Mr. Salim turned to Mr. Dulaimi, a Sunni who converted to the Shiite branch of the faith while studying in the holy Shiite city of Najaf in 1995. Mr. Dulaimi, the report noted, was picked for the operation because he “allegedly trained in Iran on how to conduct precision, military style kidnappings.”

Those kidnappings were never carried out. But the next month, militants conducted a raid to kidnap American soldiers working at the Iraqi security headquarters in Karbala, known as the Provincial Joint Coordination Center.

The documents made public by WikiLeaks do not include an intelligence assessment as to who carried out the Karbala operation. But American military officials said after the attack that Mr. Dulaimi was the tactical commander of the operation and that his fingerprints were found on the getaway car. American officials have said he collaborated with Qais and Laith Khazali, two Shiite militant leaders who were captured after the raid along with a Hezbollah operative. The Khazali brothers were released after the raid as part of an effort at political reconciliation and are now believed to be in Iran.

The documents, however, do provide a vivid account of the Karbala attack as it unfolded.

At 7:10 p.m., several sport utility vehicles of the type typically used by the American-led coalition blocked the entrance to the headquarters compound. Twenty minutes later, an “unknown number of personnel, wearing American uniforms and carrying American weapons attacked the PJCC,” the report said.

The attackers managed to kidnap four American soldiers, dragging them into an S.U.V., which was pursued by police officers from an Iraqi SWAT unit. Calculating that they were trapped, the militants shot the handcuffed hostages and fled. Three of the American soldiers who had been abducted died at the scene. The fourth later died of his wounds, the report said, and a fifth American soldier was killed in the initial attack on the compound.

Summing up the episode, the American commander of a police training team noted in the report that that the adversary appeared to be particularly well trained. “PTT leader on ground stated insurgents were professionals and appeared to have a well planned operation,” the report said.

Tue Jul 27, 2010

Leaked documents show military is paying Afghan media to run friendly stories

By John Cook
http://news.yahoo.com/

Buried among the 92,000 classified documents released by WikiLeaks yesterday is some intriguing evidence that the U.S. military in Afghanistan has adopted a PR strategy that got it into trouble in Iraq: Paying local media outlets to run friendly stories.

Several reports from Army psychological operations units and Provincial Reconstruction Teams--civilian-military hybrids tasked with rebuilding Afghanistan--show that local Afghan radio stations were under contract to air content produced by the United States. Other reports show U.S. military personnel apparently referring to Afghan reporters as "our journalists" and directing them in how to do their jobs. Such close collaboration between local media and U.S. forces has been a headache for the Pentagon in the past: In 2005, Pentagon contractor the Lincoln Group was caught paying Iraqi newspapers to run stories written by American soldiers, causing the United States considerable embarrassment.

In one of the WikiLeaks documents, a PRT member reports delivering "12 hours of PSYOP Radio Content Programming" to two radio stations in the province of Ghazni in 2008, and paying one of them "$3,900 for Radio Content Programming air time for the month of October":

The PRT provided 12 hours of PSYOP Radio Content Programming to Radio Ghaznwyan FM Station and Radio Ghazni AM/FM Station for week of 6-12 Nov. Topics included Afghanistan History, Law, and Human Rights in both Dari and Pashto, and a spreadsheet with the specific radio content programming for the week of 6-12 Nov will be forward sepcor to SPARTAN. Additionally, PRT paid Radio Ghaznwyan $3,900 for Radio Content Programming air time for the month of October

Radio Ghaznawiyaan was established and funded by the Agency for International Development, but USAID has described it in the past as a success story for local independent journalism launched with American help. So its listeners may be surprised to learn that it is an outlet for paid U.S. "PSYOP radio content."

Another message, from 2008, records a meeting that members of the Bagram PRT held with Rahimullah Samander, the news director of the Wakht News Agency and president of the Afghan Independent Journalists Association. Samander, the memo says, "proposed a partnership with the PRT" and "offered to include PRT news articles and photos on his news service":

Kapisa team met with a Kabul radio representative at the Kapisa TV and Radio Station. Met with Rahimullah Samander, news director for Wakht News Agency and president of the Afghan Independent Journalists Association. He provided information about his organizations and proposed a partnership with the PRT. He offered to include PRT news articles and photos on his news service. The PRT IO recommended a conference including Afghan and US military journalists to collaborate and share ideas. Samander hopes to increase the presence of his agency in Kapisa province.

Another 2008 memo records a similar meeting between psychological operations soldiers, Jalalabad PRT members, and representatives of Radio Television Afghanistan and the Shaiq Network. Both of these news organizations were directly contracted by psychological operations units to air friendly content:

The TF has a new PSYOP contract with RTA and a continuing PSYOP contract with Shaiq Network; additionally, these are key IO mediums. The purpose of the meetings were to introduce new HQ PSYOP members to the RTA and Shaiq managers, provide initial payment for the RTA contract, receive a PRT Advertising Campaign contract bid proposal from Shaiq (for the pending garbage removal initiative in Jalalabad), and tour both facilities.

The report, written by an Army information operations officer, describes the Afghan journalists as "very pro-CF [coalition forces]" and surmises that "there is a lot they are willing to do for the CF."

Two other messages seem to show U.S. soldiers referring to local Afghan media as extensions of their own units rather than independent reporters. In 2007, after insurgents attacked an Afghan National Police convoy, a member of Task Force Rock wrote that "we ... had our journalist conduct an interview with the Afghan National Police District Chief who condemned the attacks on their fellow countrymen." In another 2007 message, a Task Force Diablo soldier reports that after Taliban gunmen assassinated a local businessman, leading village elders to question the Afghan police's ability to keep the peace, "we were able to send the journalist in with our cultural advisor to speak to the elders."

An inquiry after the Lincoln Group revelations found that paying foreign news outlets to run friendly stories did not violate Department of Defense policy or U.S. law, though the practice seems to have been discontinued in Iraq. A Defense Department spokesperson did not immediately return an e-mail seeking comment.

On War and Words

War, Thoughts about War, Books about War

The Fog of Modern War

Published on April 7, 2010 at 3:41
http://onwarandwords.wordpress.com/

Wikileaks has acquired and decrypted (!) a copy of a tape of an Apache helicopter attacking and killing two Reuters reporters in Iraq in 2007. The Apache crew thought that the photographers were carrying weapons when what they were really carrying was camera equipment.

The video has gone truly viral by now, (predictably it has made its was to jihadist websites: here and here and here) but I strongly recommend Anthony Martinez' commentary (which is what I linked to above) on the tape. Anthony has personal experience with these sorts of engagements and offers an expert assessment on his blog. Aside from some stray mistakes that he points out, like the Wikileaks annotation not understanding what a Bradley IFV crew was saying when it said "drop ramp," and referring at one point to HMMWVs as Bradleys, he also notes that the Wikileak people failed to notice that there really was a guy in the video near the photographers with an AK and another with an RPG. Anthony rightly takes the Wikileaks people to task for not pointing out that fact. On the other hand, he also notes that he's very troubled by the fact that the Apache engaged the van that came to pick up a wounded survivor.

What do we have here? We have a non-governmental organization affecting the public debate by:

1) Engaging in activities that we would normally think of as those of intelligence agencies (acquiring the tape from an anonymous source in the US military and then figuring out how to decrypt it); and

2) Publishing a one-sided annotated version of it, at least in part because of their own technical ignorance, that is being seen around the world and negatively affecting the war effort.

While the incident had lamentable consequences (two dead reporters, two dead children, probably some other dead innocents), it does appear to have been justifiable in that there do appear to have been some bad guys present. That said, the Apache crew made a mistake in misidentifying camera equipment as weapons. This is precisely the sort of thing that Clausewitz tells us happens in war *all the time*. People make mistakes in real life and they make them even more so in wartime, when time is short, when adrenaline is flowing, when people are in danger, when people are tired, when looking at small black and white video screens, etc. (Malcolm Glad well in his book, *Blink,* has a good discussion of some of these phenomena in the context of police shootings.) The incidence of this sort of thing can be reduced but it can never be eliminated. *EVER*. Unless there is no war and I'm not going to hold my breath for that.

The problem is, that such incidents can have strategic effects. As one commenter a jihadist site put it: "After publishing this video. Some ppl in my country said 'I hate america and I support what Al-Qaeda is doing"

Welcome to modern war. Have a nice day.

The White House

Office of the Press Secretary

For Immediate Release October 07, 2011

Executive Order -- Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information

EXECUTIVE ORDER

STRUCTURAL REFORMS TO IMPROVE THE SECURITY OF CLASSIFIED NETWORKS AND THE RESPONSIBLE SHARING AND SAFEGUARDING OF CLASSIFIED INFORMATION

By the authority vested in me as President by the Constitution and the laws of the United States of America and in order to ensure the responsible sharing and safeguarding of classified national security information (classified information) on computer networks, it is hereby ordered as follows:

Section 1. Policy. Our Nation's security requires classified information to be shared immediately with authorized users around the world but also requires sophisticated and vigilant means to ensure it is shared securely. Computer networks have individual and common vulnerabilities that require coordinated decisions on risk management.

This order directs structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties. Agencies bear the primary responsibility for meeting these twin goals. These structural reforms will ensure coordinated interagency development and reliable implementation of policies and minimum standards regarding information security, personnel security, and systems security; address both internal and external security threats and vulnerabilities; and provide policies and minimum standards for sharing classified information both within and outside the Federal Government. These policies and minimum standards will address all agencies that operate or access classified computer networks, all users of classified computer networks (including contractors and others who operate or access classified computer networks controlled by the Federal Government), and all classified information on those networks.

Sec. 2. General Responsibilities of Agencies.

Sec. 2.1. The heads of agencies that operate or access classified computer networks shall have responsibility for appropriately sharing and safeguarding classified information on computer networks. As part of this responsibility, they shall:

(a) designate a senior official to be charged with overseeing classified information sharing and safeguarding efforts for the agency;

(b) implement an insider threat detection and prevention program consistent with guidance and standards developed by the Insider Threat Task Force established in section 6 of this order;

(c) perform self-assessments of compliance with policies and standards issued pursuant to sections 3.3, 5.2, and 6.3 of this order, as well as other applicable policies and standards, the results of which shall be reported annually to the Senior Information Sharing and Safeguarding Steering Committee established in section 3 of this order;

(d) provide information and access, as warranted and consistent with law and section 7(d) of this order, to enable independent assessments by the Executive Agent for Safeguarding Classified Information on Computer Networks and the Insider Threat Task Force of compliance with relevant established policies and standards; and

(e) detail or assign staff as appropriate and necessary to the Classified Information Sharing and Safeguarding Office and the Insider Threat Task Force on an ongoing basis.

Sec. 3. Senior Information Sharing and Safeguarding Steering Committee.

Sec. 3.1. There is established a Senior Information Sharing and Safeguarding Steering Committee (Steering Committee) to exercise overall responsibility and ensure senior-level accountability for the coordinated interagency development and implementation of policies and standards regarding the sharing and safeguarding of classified information on computer networks.

Sec. 3.2. The Steering Committee shall be co-chaired by senior representatives of the Office of Management and Budget and the National Security Staff. Members of the committee shall be officers of the United States as designated by the heads of the Departments of State, Defense, Justice, Energy, and Homeland Security, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the Information Security Oversight Office within the National Archives and Records Administration (ISOO), as well as such additional agencies as the co-chairs of the Steering Committee may designate.

Sec. 3.3. The responsibilities of the Steering Committee shall include:

(a) establishing Government-wide classified information sharing and safeguarding goals and annually reviewing executive branch successes and shortcomings in achieving those goals;

(b) preparing within 90 days of the date of this order and at least annually thereafter, a report for the President assessing the executive branch's successes and shortcomings in sharing and safeguarding classified information on computer networks and discussing potential future vulnerabilities;

(c) developing program and budget recommendations to achieve Government-wide classified information sharing and safeguarding goals;

(d) coordinating the interagency development and implementation of priorities, policies, and standards for sharing and safeguarding classified information on computer networks;

(e) recommending overarching policies, when appropriate, for promulgation by the Office of Management and Budget or the ISOO;

(f) coordinating efforts by agencies, the Executive Agent, and the Task Force to assess compliance with established policies and standards and recommending corrective actions needed to ensure compliance;

(g) providing overall mission guidance for the Program Manager-Information Sharing Environment (PM-ISE) with respect to the functions to be performed by the Classified Information Sharing and Safeguarding Office established in section 4 of this order; and

(h) referring policy and compliance issues that cannot be resolved by the Steering Committee to the Deputies Committee of the National Security Council in accordance with Presidential Policy Directive/PPD-1 of February 13, 2009 (Organization of the National Security Council System).

Sec. 4. Classified Information Sharing and Safeguarding Office.

Sec. 4.1. There shall be established a Classified Information Sharing and Safeguarding Office (CISSO) within and subordinate to the office of the PM-ISE to provide expert, fulltime, sustained focus on responsible sharing and safeguarding of classified information on computer networks. Staff of the CISSO shall include detailees, as needed and appropriate, from agencies represented on the Steering Committee.

Sec. 4.2. The responsibilities of CISSO shall include:

(a) providing staff support for the Steering Committee;

(b) advising the Executive Agent for Safeguarding Classified Information on Computer Networks and the Insider Threat Task Force on the development of an effective program to monitor compliance with established policies and standards needed to achieve classified information sharing and safeguarding goals; and

(c) consulting with the Departments of State, Defense, and Homeland Security, the ISOO, the Office of the Director of National Intelligence, and others, as appropriate, to ensure consistency with policies and standards under Executive Order 13526 of December 29, 2009, Executive Order 12829 of January 6, 1993, as amended, Executive Order 13549 of August 18, 2010, and Executive Order 13556 of November 4, 2010.

Sec. 5. Executive Agent for Safeguarding Classified Information on Computer Networks.

Sec. 5.1. The Secretary of Defense and the Director, National Security Agency, shall jointly act as the Executive Agent for Safeguarding Classified Information on Computer Networks (the "Executive Agent"), exercising the existing authorities of the Executive Agent and National Manager for national security systems, respectively, under National Security Directive/NSD-42 of July 5, 1990, as supplemented by and subject to this order.

Sec. 5.2. The Executive Agent's responsibilities, in addition to those specified by NSD-42, shall include the following:

(a) developing effective technical safeguarding policies and standards in coordination with the Committee on National Security Systems (CNSS), as re-designated by Executive Orders 13286 of February 28, 2003, and 13231 of October 16, 2001, that address the safeguarding of classified information within national security systems, as well as the safeguarding of national security systems themselves;

(b) referring to the Steering Committee for resolution any unresolved issues delaying the Executive Agent's timely development and issuance of technical policies and standards;

(c) reporting at least annually to the Steering Committee on the work of CNSS, including recommendations for any changes needed to improve the timeliness and effectiveness of that work; and

(d) conducting independent assessments of agency compliance with established safeguarding policies and standards, and reporting the results of such assessments to the Steering Committee.

Sec. 6. Insider Threat Task Force.

Sec. 6.1. There is established an interagency Insider Threat Task Force that shall develop a Government-wide program (insider threat program) for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels, as well as the distinct needs, missions, and systems of individual agencies. This program shall include development of policies, objectives, and priorities for establishing and integrating security, counterintelligence, user audits and monitoring, and other safeguarding capabilities and practices within agencies.

Sec. 6.2. The Task Force shall be co-chaired by the Attorney General and the Director of National Intelligence, or their designees. Membership on the Task Force shall be composed of officers of the United States from, and designated by the heads of, the Departments of State, Defense, Justice, Energy, and Homeland Security, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the ISOO, as well as such additional agencies as the co-chairs of the Task Force may designate. It shall be staffed by personnel from the Federal Bureau of Investigation and the Office of the National Counterintelligence Executive

(ONCIX), and other agencies, as determined by the co-chairs for their respective agencies and to the extent permitted by law. Such personnel must be officers or full-time or permanent part-time employees of the United States. To the extent permitted by law, ONCIX shall provide an appropriate work site and administrative support for the Task Force.

Sec. 6.3. The Task Force's responsibilities shall include the following:

(a) developing, in coordination with the Executive Agent, a Government-wide policy for the deterrence, detection, and mitigation of insider threats, which shall be submitted to the Steering Committee for appropriate review;

(b) in coordination with appropriate agencies, developing minimum standards and guidance for implementation of the insider threat program's Government-wide policy and, within 1 year of the date of this order, issuing those minimum standards and guidance, which shall be binding on the executive branch;

(c) if sufficient appropriations or authorizations are obtained, continuing in coordination with appropriate agencies after 1 year from the date of this order to add to or modify those minimum standards and guidance, as appropriate;

(d) if sufficient appropriations or authorizations are not obtained, recommending for promulgation by the Office of Management and Budget or the ISOO any additional or modified minimum standards and guidance developed more than 1 year after the date of this order;

(e) referring to the Steering Committee for resolution any unresolved issues delaying the timely development and issuance of minimum standards;

(f) conducting, in accordance with procedures to be developed by the Task Force, independent assessments of the adequacy of agency programs to implement established policies and minimum standards, and reporting the results of such assessments to the Steering Committee;

(g) providing assistance to agencies, as requested, including through the dissemination of best practices; and

(h) providing analysis of new and continuing insider threat challenges facing the United States Government.

Sec. 7. General Provisions. (a) For the purposes of this order, the word "agencies" shall have the meaning set forth in section 6.1(b) of Executive Order 13526 of December 29, 2009.

(b) Nothing in this order shall be construed to change the requirements of Executive Orders 12333 of December 4, 1981, 12829 of January 6, 1993, 12968 of August 2, 1995, 13388 of October 25, 2005, 13467 of June 30, 2008, 13526 of December 29, 2009, 13549 of August 18, 2010, and their successor orders and directives.

(c) Nothing in this order shall be construed to supersede or change the authorities of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended; the Secretary of Defense under Executive Order 12829, as amended; the Secretary of Homeland Security under Executive Order 13549; the Secretary of State under title 22, United States Code, and the Omnibus Diplomatic Security and Antiterrorism Act of 1986; the Director of ISOO under Executive Orders 13526 and 12829, as amended; the PM-ISE under Executive Order 13388 or the Intelligence Reform and Terrorism Prevention Act of 2004, as amended; the Director, Central Intelligence Agency under NSD-42 and Executive Order 13286, as amended; the National Counterintelligence Executive, under the Counterintelligence Enhancement Act of 2002; or the Director of National Intelligence under the National Security Act of 1947, as amended, the Intelligence Reform and Terrorism Prevention Act of 2004, as amended, NSD-42, and Executive Orders 12333, as amended, 12968, as amended, 13286, as amended, 13467, and 13526.

(d) Nothing in this order shall authorize the Steering Committee, CISSO, CNSS, or the Task Force to examine the facilities or systems of other agencies, without advance consultation with the head of such agency, nor to collect information for any purpose not provided herein.

(e) The entities created and the activities directed by this order shall not seek to deter, detect, or mitigate disclosures of information by Government employees or contractors that are lawful under and protected by the Intelligence Community Whistleblower Protection Act of 1998, Whistleblower Protection Act of 1989, Inspector General Act of 1978, or similar statutes, regulations, or policies.

(f) With respect to the Intelligence Community, the Director of National Intelligence, after consultation with the heads of affected agencies, may issue such policy directives and guidance as the Director of National Intelligence deems necessary to implement this order.

(g) Nothing in this order shall be construed to impair or otherwise affect:

(1) the authority granted by law to an agency, or the head thereof; or

(2) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals

(h) This order shall be implemented consistent with applicable law and appropriate protections for privacy and civil liberties, and subject to the availability of appropriations.

(i) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA

THE WHITE HOUSE,
October 7, 2011.

The White House

Office of the Press Secretary

For Immediate Release October 07, 2011

Fact Sheet: Safeguarding the U.S. Government's Classified Information and Networks

Following the unlawful disclosure of classified information by WikiLeaks in the summer of 2010, the National Security Staff formed an interagency committee to review the policies and practices surrounding the handling of classified information, and to recommend government-wide actions to reduce the risk of a future breach. Since then, this effort has been a top priority of the Administration and senior agency officials have been actively engaged in developing policies and oversight mechanisms to enhance our national security through responsible sharing and safeguarding of classified information.

The strategic imperative of our efforts has been to ensure that we provide adequate protections to our classified information while at the same time sharing the information with all who reasonably need it to do their jobs. The guiding principles during the Administration's review were to:

- Reinforce the importance of responsible information sharing and not undo all of the significant and important progress we've made in interagency information sharing since 9/11;
- Ensure that policies, processes, technical security solutions, oversight, and organizational cultures evolve to match our information sharing and safeguarding requirements;
- Emphasize that effective and consistent guidance and implementation must be coordinated across the entire Federal government. We are only as strong as our weakest link and this is a shared risk with shared responsibility; and;
- Continue to respect the privacy, civil rights, and civil liberties of the American people.

The committee that was established in the wake of WikiLeaks proposed a new oversight structure to orchestrate the development and implementation of policies and standards for the sharing and safeguarding of classified information on computer networks. These structural reforms are reflected in the Executive Order signed today by President Obama.

In accordance with today's Executive Order:

- **Agencies bear the primary responsibility** for sharing and safeguarding classified information, consistent with appropriate protections for privacy and civil liberties. Federal agencies that use classified networks will:

- designate a senior official to oversee classified information sharing and safeguarding for the agency;
- implement an insider threat detection and prevention program; and
- perform self assessments of compliance with policy and standards.

- A **Senior Information Sharing and Safeguarding Steering Committee** will have overall responsibility for fully coordinating interagency efforts and ensuring that Departments and Agencies are held accountable for implementation of information sharing and safeguarding policy and standards.
- A **Classified Information Sharing and Safeguarding Office** will be created within the office of the Program Manager for the Information Sharing Environment to provide sustained, full-time focus on sharing and safeguarding of classified national security information. The office will also consult partners to ensure the consistency of policies and standards and seek to identify the next potential problem.
- Senior representatives of the Department of Defense and the National Security Agency will jointly act as the **Executive Agent for Safeguarding Classified Information on Computer Networks** to develop technical safeguarding policies and standards and conduct assessments of compliance.
- An **Insider Threat Task Force** will develop a government-wide program for insider threat detection and prevention to improve protection and reduce potential vulnerabilities of classified information from exploitation, compromise or other unauthorized disclosure.

We did not, however, wait for today's Executive Order to begin taking steps. The Senior Information Sharing and Safeguarding Steering Committee formally established today began meeting informally in June to track steps taken across the Federal Government. In addition to those measures identified in today's Executive Order, significant progress has been made by U.S. Departments and Agencies in five priority areas:

1. **Removable media**

Departments and Agencies have made significant progress in clarifying and standardizing removable media policies, processes, and technical controls. We have limited the numbers of users with removable media permissions and strengthened accountability for violations.

2. **Online Identity Management**

The owners and operators of classified systems are accelerating efforts to strengthen the online verification of individuals logging on to classified systems, and to be able to track what information is being accessed by these individuals.

3. **Insider Threat Program**

As directed in the Executive Order, the Attorney General and the Director of National Intelligence are actively establishing an interagency Insider Threat Task Force. This Task Force will integrate specialized abilities, tools, and techniques to more effectively deter, detect, and disrupt the insider threat.

4. **Access control**

Departments and Agencies are implementing more robust access control systems to enforce role-based access privileges that serve to ensure that an individual user's information access is commensurate with his/her assigned role.

5. **Enterprise audit**

Enhancing auditing capabilities across U.S. Government classified networks is a priority effort, and planning has been initiated to define the policy and develop standards for the collection and sharing of audit and insider threat data.

Joint Statement for the Record

Senate Homeland Security and Government Affairs Committee

Hearing on Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration

March 10, 2011

Ms. Teresa Takai
Chief Information Officer and
Acting Assistant Secretary of Defense for Networks and Information Integration

Mr. Thomas Ferguson
Principal Deputy Under Secretary of Defense for Intelligence

Chairman Lieberman, Ranking Member Collins and distinguished Members of the Committee, thank-you for the invitation to provide testimony on what the Department of Defense (DoD) is doing to improve the security of its classified networks while ensuring that information is shared effectively.

The 9/11 attacks and their aftermath revealed gaps in intra-governmental information sharing. Departments and agencies have taken significant steps to reduce those obstacles, and the work that has been done to date has resulted in considerable improvement in information sharing and increased cooperation across government operations. However, as we have now seen with the WikiLeaks compromises, these efforts to give diplomatic, military, law enforcement and intelligence specialists quicker and easier access to greater amounts of information have made our sensitive data more vulnerable to compromise. The expanded use of computer networks has also increased the opportunity for even a single authorized user to access, copy, manipulate, download, and intentionally publicize enormous amounts of information from the interconnected databases of multiple agencies. As part of an integrated federal government approach, DoD has taken and continues to take steps to prevent such compromises from happening again.

SIPRNet - Background

Before discussing the particulars of the WikiLeaks incident and the exfiltration of classified documents from the DoD Secret Internet Protocol Router Network (SIPRNet), we would like to first provide a brief overview of the SIPRNet and explain why classified information is widely shared on this network and others like it.

In the mid-1990s, DoD created a network that functions like a classified internet. This network, called SIPRNet, is principally used as a means of posting and sharing essential command and control, mission planning and execution, and intelligence information – particularly among war fighters and command headquarters. Every SIPRNet connection is physically protected and cryptographically isolated, and each authorized user must have a SECRET-level clearance. SIPRNet connects approximately two thousand DoD locations and has between 400,000 and 500,000 DoD users.

One can think of SIPRNet as a classified DoD internet that connects DoD classified local area networks with each other and with classified networks across the government. Each local area network hosts its own organization's classified information services on SIPRNet and selects which elements of its information to make accessible to the larger network. Most information is made available on web pages supported by

search engines. A search on a subject will return links to information available on any Department or Agency network connected to SIPRNet that grants the authorized searcher access to that data.

WikiLeaks Disclosures and Immediate DoD Actions

In late July 2010, Wikileaks released thousands of classified DoD documents related to the War in Afghanistan – the first disclosure of several to follow. In late October 2010, Wikileaks released 400,000 classified Iraq logs, and in late November 2010 Wikileaks began an ongoing release of State Department diplomatic cables.

On August 12, 2010, immediately following the first release of documents, the Secretary of Defense commissioned two internal DoD studies. The first study, led by the Under Secretary of Defense for Intelligence (USD(I)), directed a review of DoD information security policy. The second study, led by the Joint Staff, focused on procedures for handling classified information in forward deployed areas. The Secretary also tasked the Director of the Defense Intelligence Agency to stand up an Information Review Task Force to assess, in concert with interagency participants, the substance of the data disclosed.

Results of the two studies revealed a number of findings, including the following:

- Forward deployed units maintained an over-reliance on removable electronic storage media.
- Roles and responsibilities for detecting and dealing with an insider threat must be better defined.
- Processes for reporting security incidents need improvement.
- Limited capability currently exists to detect and monitor anomalous behavior on classified computer networks.

Once the studies were concluded and the results reported to the Secretary, the Department began working to address the findings and improve its overall security posture to mitigate the possibility of another similar type of disclosure. Some of this work was already planned or underway. For other findings, like the issue of removable media, new initiatives had to be immediately implemented.

DoD Technical Mitigations Efforts

The most expedient remedy for the vulnerability that led to the WikiLeaks disclosure was to prevent the ability to remove large amounts of data from the classified network. This recommendation, forwarded in both the USD(I) and Joint Staff assessments, considered the operational impact of severely limiting users' ability to move data from SIPRNet to other networks (such as coalition networks) or to weapons platforms. The impact was determined to be acceptable if a small number of computers retained the ability to write to removable media for operational reasons and under strict controls.

The preferred method to accomplish this was by means of security software the Department is deploying to all of its workstations – the Host Based Security System (HBSS). HBSS provides very positive technical control over the machines and reports on machine configurations which can be centrally monitored. In this particular case the Device Control Module (DCM) on HBSS is used to disable the use of removable media. For those few machines where writing is allowed HBSS will report, in real time, each write operation. It will also report every attempt of an unauthorized write operation. Where HBSS is not yet fully deployed other means are used to disable write capability, such as removing the software used to write to CDs, removing the drives themselves from the machines, or blocking access to external devices in workstation configuration files.

The Department has completed disabling the write capability on all of its SIPRNet machines except for the few – currently about 12% – that maintain that capability for operational reasons. The great majority of these are disabled using HBSS, so we have positive visibility into their status. We will complete installation of HBSS on SIPRNet in June 2011. The machines that maintain write capability for operational reasons are enabled under strict controls, such as using designated kiosks with two-person controls.

DoD Policy Review

Not all of the actions necessary to ensure information security are focused on technical solutions. The Defense Security Service (DSS) is developing web-enabled information security training that will become part of the mandatory information assurance training conducted annually across the Department. Five separate policies are now combined in an updated version of DoD's Information Security Program policy.

Some examples of work already underway include last year's stand-up of the first defense security oversight and assessment program. The program reaches out to defense components to understand strategic issues for the enterprise, highlight best practices, and monitor compliance with DoD security policy. In addition, the Joint Staff is establishing an oversight program that will include inspection of forward deployed areas.

To establish better governance over cross-functional responsibilities for insider threats, the Assistant Secretary of Defense for Homeland Defense and America's Security Affairs (ASD(HD&ASA)) was appointed the lead across the Department for standing up a formal insider threat program. ASD(HD&ASA) is developing a concept of operations which will ultimately be briefed to the Secretary.

Access Controls

One of the major contributing factors in the WikiLeaks incident was the large amount of data that was accessible with little or no access controls. Broad access to information can be combined with access controls in order to mitigate this vulnerability. While there are many sites on SIPRNet that do have access controls, these are mostly password-based and therefore do not scale well. The administration of thousands of passwords is labor intensive and it is difficult to determine who should (and should not) have access.

DoD has begun to issue a Public Key Infrastructure (PKI)-based identity credential on a hardened smart card. This is very similar to the Common Access Card (CAC) we use on our unclassified network. We will complete issuing 500,000 cards to our SIPRNet users, along with card readers and software, by the end of 2012. This will provide very strong identification of the person accessing the network and requesting data. It will both deter bad behavior and require absolute identification of who is accessing data and managing that access.

In conjunction with this, all DoD organizations will configure their SIPRNet-based systems to use the PKI credentials to strongly authenticate end-users who are accessing information in the system. This provides the link between end users and the specific data they can access – not just network access. This should, based on our experience on the unclassified networks, be straightforward.

DoD's goal is that by 2013, following completion of credential issuance, all SIPRNet users will log into their local computers with their SIPRNet PKI/smart card credential. This will mirror what we already do on the unclassified networks with CACs.

Our intention is for all SIPRNet web servers to require PKI credentials by mid-2013, again mirroring what's been done on our unclassified network. Beyond that, DoD components will modify all other SIPRNet systems to use the SIPRNet PKI credential for access control.

More sophisticated access control is possible as the technology enables the linkage of identification with organizational and user roles (e.g., knowing someone is a CENTCOM intelligence analyst). Information services can then make access control decisions "on-the-fly" without having pre-arranged user accounts – the system positively identifies the user's identity, attributes and role. This allows better information access by unanticipated users, and more agility in the way DoD missions are done.

However, it is very important to note that while the technology can provide for very specific access controls, it will be difficult to (1) categorize the many different roles and (2) decide what information should be accessible to users performing in those roles. The technology will make it possible to determine who is accessing what, make it much easier to audit activity, and to control access based on identity and role. However, while this can make it possible to prevent the "financial analyst" from accessing large amounts of intelligence data, the general intelligence analyst or operational planner will still need to have access to enormous amounts of data since such access is essential to successful performance of their function.

Insider Threat Detection

There are a number of working groups dealing with the insider threat problem at the interagency and DoD levels, some predating WikiLeaks, and some formed recently. For example, the National Counterintelligence Executive (NCIX) is leading efforts to establish an information technology insider detection capability and an Insider Threat program – primarily focused on the Intelligence Community. DoD counterintelligence, security and information assurance personnel are engaged in the NCIX insider threat initiatives.

As stated previously, within DoD the Secretary has designated the ASD(HD&ASA) to develop and lead a holistic DoD Insider Threat Program. To create an effective and functional program to protect the DoD, the four primary components - Counterintelligence, Information Assurance, Antiterrorism/Force Protection and Security – must work in partnership; the emerging DoD Insider Threat program will drive that integration. A plan is being developed for a DoD-wide IT audit, monitoring and analysis capability to identify suspicious behavior on all DoD information systems. As an

element of the DoD Insider Threat Program, USD(I) has been developing comprehensive policy for a DoD CI Insider Threat Program to detect, identify, assess, exploit and deny insider threats that have a foreign nexus, and that may lead to espionage and support to international terrorism. The DoD CI Insider Threat program activities can also identify other individuals who pose a potential insider threat but are not linked to foreign intelligence services or international terrorist organizations. DoD CI personnel will forward such information to the appropriate officials. Policy for the CI Insider Threat program is in coordination. The Director of DIA, the DoD CI Manager, has taken the functional lead for CI Insider Threat for the DoD CI community. He has directed the DoD Insider Threat CI Group to assist the DoD Components in establishing CI Insider Threat programs, identifying best practices and providing functional guidance.

Our strategy on tools is to examine a variety of Insider Threat detection technologies and employ them where they are most appropriate. One very promising capability is the Audit Extraction Module (AEM) developed by the National Security Agency (NSA). This software leverages already existing audit capabilities and reports to the network operators on selected audit events that indicate questionable behavior. A great advantage is that it can be integrated into the HBSS we have already installed on the network, and so deployment should be relatively inexpensive and timely. AEM is being integrated into HBSS now and will be operationally piloted this summer.

Commercial counterintelligence and law enforcement tools – mostly used by the intelligence community – are also being examined and will be a part of the overall DoD insider threat program. These tools provide much more capability than the AEM. However, while currently in use in some agencies, they are expensive to deploy and sustain even when used in small, homogeneous networks. Widespread deployment in DoD will be a challenge. The Army is working on piloting one of these tools on parts of their intelligence networks and this should give us some good data on cost and utility.

In support of this activity we are employing our Enterprise Software Initiative to put in place a contract vehicle to support acquisition both for existing and future insider threat detection tools. The contract – a basic purchasing agreement – should be in place by June 2011.

Improving Information Sharing and Protection

As DoD continues to move forward with improving our information sharing capabilities, we will continue to concurrently improve our posture and mechanisms to protect intelligence information without reverting back to pre-9/11 stovepipes. DoD is

currently involved in multiple interagency level working groups designed to identify specific strategies to improve intelligence information sharing while ensuring the appropriate protection and safeguards are in place. Solving these problems will require a multi-disciplinary, whole of government approach, which DoD is helping solve by conducting a review of our own practices and identifying lessons learned. DoD's mission and extensive experience in dealing with complex sharing issues with foreign and domestic partners provides unique perspectives and will serve as a reference for our plans.

One of the immediate results from these interagency level discussions is the highlighted need for stronger coherence among the various policies governing the dissemination and handling of classified national security information, including intelligence, across the Government. DoD agrees with the DNI that responsible information sharing must include mechanisms to safeguard intelligence while protecting valuable sources and methods. The Department believes this is an inherent responsibility of every individual using the network. This dual responsibility to share and protect information requires a comprehensive approach including coherent policies, responsive architectures, better tools for sharing and protecting, effective training and education, uniform cultural behaviors underpinned with strong, proactive, responsible leadership.

The activities we already have underway to improve information sharing will inherently improve our ability to protect. Increased emphasis on user authentication, data tagging, development of user attributes, and implementation of advanced technologies such as Cloud implementations, consolidated discovery, and single-sign on will provide the foundational technology that will continue to improve sharing and data discovery while bringing protection up to the same level.

Conclusion

The full impact of the WikiLeaks disclosures may not be evident for some time. It is clear, however, that the unauthorized release of U.S. information by WikiLeaks has adversely affected our global engagement and national security and endangered the lives of individuals who have sought to cooperate with the United States. It is of vital importance to DoD and the entire U.S. Government that we keep our sensitive and classified information secure, while at the same time ensuring that the right people have the timely access they need to help keep our country and its citizens safe. We appreciate the Committee's attention to this important issue, and look forward to a continued dialogue as we move forward together.

FOR IMMEDIATE RELEASE October 7, 2011

Statement by National Archives Information Security Oversight Office (ISOO) Director John Fitzpatrick

Today President Obama signed an Executive Order entitled "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information."

I applaud the President's leadership in energizing and fortifying executive branch efforts to ensure that standards for sharing and safeguarding classified national security information are implemented. This Executive Order recognizes that the primary responsibility lies with departments and agencies to carry out this initiative, while it also reinforces the responsibilities of individuals entrusted with access to classified information.

The structural reforms required by this Order will enable agencies to share information more securely. Strengthening standards and practices of protection will lead to greater trust and cooperation and increased information sharing.

As the government entity charged with overseeing executive branch performance in executing the President's program for classified information, ISOO commends this renewed emphasis on improving implementation of safeguarding standards. I look forward to continued participation in the development of national policies and standards that will ensure consistent application of sharing and safeguarding practices across government.

John Fitzpatrick
Director
Information Security Oversight Office
National Archives and Records Administration

* * *

For press information, contact the National Archives Public Affairs staff at 202-357-5300.

12-11

WIRED
July 6, 2010

Army Intelligence Analyst Charged With Leaking Classified Information
By Kim Zetter and Kevin Poulsen

A U.S. Army intelligence analyst suspected of leaking videos and documents to Wikileaks was charged Monday with eight violations of federal criminal law, including unauthorized computer access, and transmitting classified information to an unauthorized third party.

Pfc. Bradley Manning, 22, was charged with two counts under the Uniform Code of Military Justice: one encompassing the eight alleged criminal offenses, and a second detailing four noncriminal violations of Army regulations governing the handling of classified information and computers.

According to the charge sheet, Manning downloaded a classified video of a military operation in Iraq and transmitted it to a third party, in violation of a section of the Espionage Act, 18 U.S.C. 793(e), which involves passing classified information to an uncleared party, but not a foreign government.

The remaining criminal charges are for allegedly abusing access to the Secret-level SIPR network to obtain more than 150,000 U.S. State Department cables, as well as an unspecified classified PowerPoint presentation.

Manning allegedly passed more than 50 classified diplomatic cables to an unauthorized party, but downloaded at least 150,000 unclassified State Department documents, according to Army spokesman Lt. Col. Eric Bloom. These numbers could change as the investigation continues, Bloom said. Both numbers are lower than the 260,000 cables Manning claimed, in online chats, to have passed to Wikileaks.

Between Jan. 13 and Feb. 19 this year, Manning allegedly passed one of the cables, titled "Reykjavik 13," to an unauthorized party, the Army states. The Army doesn't name Wikileaks as the recipient of the document, but last February the site published a classified cable titled "Reykjavik 9″ that describes a U.S. embassy meeting with the government of Iceland.

If convicted of all charges, Manning could face a prison sentence of as much as 52 years, Bloom said.

Manning was put under pretrial confinement at the end of May, after he disclosed to a former hacker that he was responsible for leaking classified information to Wikileaks. He's currently being held at Camp Arifjan in Kuwait and has been assigned a military defense attorney, Capt. Paul Bouchard, who was not available for comment. Bloom said that Manning has not retained a civilian attorney, though Wikileaks stated recently that it commissioned unnamed attorneys to defend the soldier.

The next step in Manning's case is an Article 32 hearing, which is an evidentiary hearing similar to a grand jury hearing, to determine if the case should proceed to court-martial.

Manning, who comes from Potomac, Maryland, enlisted in the Army in 2007 and was an Army intelligence analyst who was stationed at Forward Operating Base Hammer 40 miles east of Baghdad, Iraq, last November. He held a Top Secret/SCI clearance.

In May, he began communicating online with a former hacker named Adrian Lamo. Very quickly in his exchange with the ex-hacker, Manning disclosed that he was responsible for leaking a headline-making

Army video to Wikileaks. The classified video, which Wikileaks released April 5 under the title "Collateral Murder," depicted a deadly 2007 U.S. helicopter air strike in Baghdad on a group of men, some of whom were armed, that the soldiers believed were insurgents.

The attack killed two Reuters employees and an unarmed Baghdad man who stumbled on the scene afterward and tried to rescue one of the wounded by pulling him into his van. The man's two children were in the van and suffered serious injuries in the hail of gunfire.

Manning also said he leaked a separate video to Wikileaks showing the notorious May 2009 air strike near Garani village in Afghanistan that the local government says killed nearly 100 civilians, most of them children. The Pentagon released a report about the incident last year, but backed down from a plan to show video of the attack to reporters.

Other classified leaks he claimed credit for included an Army document evaluating Wikileaks as a security threat and a detailed Army chronology of events in the Iraq war. But the most startling revelation was a claim that he gave Wikileaks a database of 260,000 classified U.S. diplomatic cables, which Manning said exposed "almost-criminal political back dealings."

"Hillary Clinton and several thousand diplomats around the world are going to have a heart attack when they wake up one morning, and find an entire repository of classified foreign policy is available, in searchable format, to the public," Manning told Lamo in an online chat session.

Manning anticipated watching from the sidelines as his action bared the secret history of U.S. diplomacy around the world.

"Everywhere there's a U.S. post, there's a diplomatic scandal that will be revealed," Manning wrote of the cables. "It's open diplomacy. Worldwide anarchy in CSV format. It's Climategate with a global scope, and breathtaking depth. It's beautiful, and horrifying."

Wikileaks has acknowledged possessing the Afghanistan video and representatives of the organization indicated in media interviews that it will release the video soon. The organization has denied that it received 260,000 classified cables.

In his chats with Lamo, Manning discussed personal issues that got him into trouble with his Army superiors and left him socially isolated, and said he had been demoted and was headed for an early discharge from the military.

He claimed to have been rummaging through classified military and government networks for more than a year and said the networks contained "incredible things, awful things … that belonged in the public domain, and not on some server stored in a dark room in Washington, D.C."

Manning discovered the Iraq video in late 2009, he said. He first contacted Wikileaks founder Julian Assange sometime around late November last year, he claimed, after Wikileaks posted 500,000 pager messages covering a 24-hour period surrounding the Sept. 11 terror attacks. "I immediately recognized that they were from an NSA database, and I felt comfortable enough to come forward," he wrote to Lamo.

In January, while on leave in the United States, Manning visited a close friend in Boston and confessed he'd gotten his hands on unspecified sensitive information, and was weighing leaking it, according to the friend. "He wanted to do the right thing," 20-year-old Tyler Watkins told Wired.com. "That was something I think he was struggling with."

Manning passed the video to Wikileaks in February, he told Lamo. After April 5 when the video was released and made headlines, Manning contacted Watkins from Iraq asking him about the reaction in the United States.

"He would message me, 'Are people talking about it?… Are the media saying anything?'" Watkins said. "That was one of his major concerns, that once he had done this, was it really going to make a difference?… He didn't want to do this just to cause a stir…. He wanted people held accountable and wanted to see this didn't happen again."

Lamo decided to turn in Manning after the soldier told him that he leaked a quarter-million classified embassy cables. Lamo contacted the Army, and then met with Army CID investigators and the FBI to pass the agents a copy of the chat logs from his conversations with Manning. At their second meeting with Lamo on May 27, FBI agents from the Oakland Field Office told the hacker that Manning had been arrested the day before in Iraq by Army CID investigators.

As described by Manning in his chats with Lamo, his purported leaking was made possible by lax security online and off.

Manning had access to two classified networks from two separate secured laptops: SIPRNET, the Secret-level network used by the Department of Defense and the State Department, and the Joint Worldwide Intelligence Communications System which serves both agencies at the Top Secret/SCI level.

The networks, he said, were both "air gapped" from unclassified networks, but the environment at the base made it easy to smuggle data out.

"I would come in with music on a CD-RW labeled with something like 'Lady Gaga,' erase the music then write a compressed split file," he wrote. "No one suspected a thing and, odds are, they never will."

"[I] listened and lip-synced to Lady Gaga's 'Telephone' while exfiltrating possibly the largest data spillage in American history," he added later. "Weak servers, weak logging, weak physical security, weak counterintelligence, inattentive signal analysis … a perfect storm."

Manning told Lamo that the Garani video was left accessible in a directory on a U.S. Central Command server, centcom.smil.mil, by officers who investigated the incident. The video, he said, was an encrypted AES-256 ZIP file.

http://www.wired.com/threatlevel/2010/07/manning-charges/#

The Telegraph (UK)
30 July 2010

Bradley Manning, suspected source of Wikileaks documents, raged on his Facebook page
By Heidi Blake, John Bingham and Gordon Rayner

The US Army intelligence analyst, who is half British and went to school in Wales, appeared to sink into depression after a relationship break-up, saying he didn't "have anything left" and was "beyond frustrated".

In an apparent swipe at the army, he also wrote: "Bradley Manning is not a piece of equipment," and quoted a joke about "military intelligence" being an oxymoron.

Mr Manning, 22, who is currently awaiting court martial, is suspected of leaking more than 90,000 secret military documents to the Wikileaks website in a security breach which US officials claim has endangered the lives of serving soldiers and Afghan informers.

Supporters claim the war logs leak exposed civilian deaths in Afghanistan which had been covered up by the military, and Mr Manning's family, who live in Pembrokeshire, said he had "done the right thing".

The Pentagon, which is investigating the source of the leak, is expected to study Mr Manning's background to ascertain if they missed any warnings when he applied to join the US Army. The postings on his Facebook page are also likely to form part of the inquiry.

Mr Manning, who is openly homosexual, began his gloomy postings on January 12, saying: "Bradley Manning didn't want this fight. Too much to lose, too fast."

At the beginning of May, when he was serving at a US military base near Baghdad, he changed his status to: "Bradley Manning is now left with the sinking feeling that he doesn't have anything left."

Five days later he said he was "livid" after being "lectured by ex-boyfriend", then later the same day said he was "not a piece of equipment" and was "beyond frustrated with people and society at large".

His tagline on his personal page reads: "Take me for who I am, or face the consequences!"

Mr Manning was arrested at the end of May on suspicion of leaking a video of a US helicopter attack, and quickly became the main suspect when the Afghan war documents were leaked earlier this week.

His uncle, Kevin Fox, said the soldier's arrest and imprisonment in a military jail had taken its toll on his mother Susan, who lives in Haverfordwest.

"She hasn't been well," he said, adding that if Mr Manning had leaked the documents: "I think the boy did the right thing."

Another close relative, who asked not to be named, said: "His mum didn't know anything about what he was doing and it's come as a big shock. She's very upset."

Susan Manning, 56, moved to the US in 1979 after marrying Bradley's American father Brian Manning, a former serviceman who was based at the Cawdor Barracks in Brawdy, near Haverfordwest.

Bradley Manning was born in Oklahoma but the couple divorced in 2001 and Mrs Manning moved back to Wales with her son, who sat his GCSEs at the Tasker Milward secondary school in Haverfordwest.

Joseph Staples, Mr Manning's uncle by marriage, said: “It's one of those Catch 22 situations, because freedom of speech is great but if you do something that endangers other people's lives then I can understand why you're going to get flattened by the American military.

“Some people are saying that Bradley was a trouble-maker but he was anything but. He was just an introverted kid who loved computers and was fired up politically.”

Scott Lewis, a former classmate, said: "He was a bit hot-headed. If there was something he didn't agree with, he spoke up about it."

Other school contemporaries recalled him as a computer “nerd” who had a difficult relationship with his father.

Jenna Morris, a 23-year-old sales manager who went on holiday to Disney World in Florida with Bradley and his cousins, said: “He was a quiet lad and he’d had a tough upbringing.

His parents had an acrimonious divorce. He didn’t get on well with his dad; they had quite a volatile relationship. His dad was very strict and shouted at him a lot.

“He had a tough time when he came back here with his mum because moving to another country after a break-up was hard. He was quite a loner and he didn’t really have a lot of friends. He had quite a bit of trouble at school and was picked on, but he didn’t care.”

James Kirkpatrick, who became friendly with him through their shared interest in computers, said: “I last contacted him about six months ago. He didn’t mention anything about what was happening, but at the same time he did seem a bit secretive, he was being a bit paranoid about what we spoke about on the net.

“He wouldn’t mention anything about what he was doing in the army and what he thought of it.”

Pictures on Mr Manning's Facebook page include photos of him on school trips during his time in Wales and at a gay rights rally, where he is holding up a placard demanding equality on "the battlefield".

Yesterday Mr Manning, who is reportedly on suicide watch, was transferred from a military jail in Kuwait to a prison in Washington DC, as the Pentagon called in the FBI to assist in the hunt for the source of the leak.

Admiral Mike Mullen, the chairman of the US military's Joint Chiefs of Staff, said the leakers “might already have on their hands the blood of some young soldier or that of an Afghan family” because, he said, the leaked documents included the names of Afghan informants.

http://www.telegraph.co.uk/news/worldnews/asia/afghanistan/7918632/Bradley-Manning-suspected-source-of-Wikileaks-documents-raged-on-his-Facebook-page.html

WIRED
September 1, 2010

Attorney: Army Disabled Manning's Weapon Prior to Leaks
By Kim Zetter

A civilian defense attorney hired recently by alleged WikiLeaks leaker Bradley Manning says the Army was so concerned about his client's mental health prior to the alleged leaks that supervisors removed the bolt from his military weapon, disabling it.

Attorney David Coombs told CNN, however, that other than sending Manning to a chaplain for counseling, the Army did little to address its concerns about him.

"The unit has in fact documented a history, if you will, from as early as December of 2009 to May of 2010 of behavior that they were concerned about," Coombs said, adding that Manning's immediate supervisor "did document prolonged periods of disassociated behavior, quite a bit of nonresponsiveness from Pfc. Manning. And, again, that progressed from the very beginning of the deployment and deteriorated somewhat toward the end."

The Army declined to comment. "This case does have worldwide visibility and [Manning's] civilian attorney will do the best he can to defend him and that may bring up other issues other than what is currently known," said Lt. Col. Robert Owen, spokesman for the Army at the U.S. embassy in Iraq. "But the U.S. Army is not going to react to every statement that Manning's civilian attorney makes."

Manning, who is being held in solitary confinement at the Marine Corps brig at Quantico, Virginia, has invoked the Fifth Amendment and is refusing to cooperate with investigators. He's taking medication for depression and insomnia. Coombs told CNN, however, that his client is aware of the public support for him.

http://www.wired.com/threatlevel/tag/bradley-manning/page/3/

WIRED
January 27, 2011

Army Was Warned Not to Deploy Bradley Manning to Iraq
By Kim Zetter

Army commanders were warned against sending to Iraq an Army private who is suspected of leaking hundreds of thousands of sensitive documents to the secret-spilling site WikiLeaks.

Pfc. Bradley Manning's supervisor at Ft. Drum in New York had told his superiors that Manning had discipline problems and had thrown chairs at colleagues and shouted at higher-ranking soldiers, according to a report by McClatchy News service.

But Manning was deployed to Iraq anyway because the Army needed his skills and was short-staffed with intelligence analysts, according to anonymous military officials who spoke with McClatchy. Manning's

superiors believed his discipline problems could be addressed in Iraq, but then they failed to properly monitor him once he got there.

The information was uncovered by a six-member taskforce that was charged with investigating how Manning was trained and whether his supervisors had made mistakes. Their report is due to be delivered to Army Secretary John McHugh by Feb. 1.

The taskforce found that although the military had followed procedures in giving Manning his security clearance, they neglected to re-assess this decision to determine whether he should have retained his clearance once he exhibited disciplinary problems.

Three officers in Manning's chain of command could face disciplinary action over their handling of the soldier, according to McClatchy.

Manning was deployed to Forward Operating Base Hammer in Iraq in late October 2009. There, he served as an intelligence analyst with a rank of Specialist and with a Top Secret/SCI clearance. He had access to classified networks, including SIPRnet, the Army's secret-level wide area network linked to WikiLeaks' most high-profile releases. He allegedly began leaking within months of being deployed.

He was arrested in Iraq in May 2010, after allegedly confessing to a former hacker in online chats that he had illegally downloaded thousands of classified and sensitive documents from classified networks and passed them to WikiLeaks. He also revealed in the chats that he had similar discipline problems in Iraq, where he had punched a colleague in the face. The action resulted in his demotion from Specialist to Private First Class shortly before his arrest.

In the chats, Manning told Lamo that he first contacted WikiLeaks' founder Julian Assange in late November 2009, after Wikileaks posted 500,000 pager messages covering a 24-hour period surrounding the September 11, 2001 terror attacks.

Manning said he had already been sifting through the classified networks for months when he discovered a classified Iraq video in late 2009. The video showed a 2007 Army helicopter attack on a group of men.

In January 2010, while on leave in the United States, Manning visited a close friend in Boston and confessed he'd gotten his hands on unspecified sensitive information, and was weighing leaking it. He allegedly then passed the video to Wikileaks in February, which published it online in April last year.

In early May, Manning was demoted after punching a colleague during an argument. "Something I never do …!?" he told Lamo.

"It was a minor incident, but it brought attention to me," he said. At this point, his life, which was already in turmoil, began to unravel as his career began to implode.

"I had about three breakdowns, successively worse, each one revealing more and more of my uncertainty and emotional insecurity," he told Lamo.

Last July, Threat Level reported that Manning's behavior had raised red flags as early as 2008 when he was still in training and before he was stationed at Ft. Drum. He was admonished then for uploading YouTube videos in which he discussing classified facilities.

Manning had enlisted in October 2007 and was only three months into his 16 weeks of training as an intelligence analyst when about 25 of his fellow recruits reported him for the videos. At the time, he had completed basic training and was receiving advanced individual training at the Army's Intelligence Center of Excellence at Fort Huachuca, Arizona.

The videos were messages that Manning shot for his family from his room at the barracks. Manning would talk about how his day was going and although he did not disclose classified information in the videos, he talked about the base's SCIFs, secure rooms where classified information is processed.

"It was brought up to his command, and his command took action on that," an official told Threat Level last July. "A lot of his actions back then, you couldn't tell it would come to what it's come to now, but it was a red flag."

Manning was ordered to remove the videos but he did not lose his then-provisional Top Secret security clearance.

http://www.wired.com/threatlevel/tag/bradley-manning/

The Washington Post
Wednesday, March 2, 2011; 9:34 PM

Army charges WikiLeaks suspect with 'aiding enemy'
by ROBERT BURNS
The Associated Press

WASHINGTON -- An Army private suspected of leaking hundreds of thousands of sensitive and classified documents to the WikiLeaks anti-secrecy group was charged Wednesday with aiding the enemy, a crime that can bring the death penalty or life in prison.

The Army filed 22 new charges against Pvt. 1st Class Bradley E. Manning, including causing intelligence information to be published on the Internet. The charges don't specify which documents, but the charges involve the suspected distribution by the military analyst of more than 250,000 confidential State Department cables as well as a raft of Iraq and Afghanistan war logs. Thousands of the documents have been published on the WikiLeaks website.

Although aiding the enemy is a capital offense under the Uniform Code of Military Justice, Army prosecutors have notified the Manning defense team that it will not recommend the death penalty to the two-star general who is in charge of proceeding with legal action.

The Army has not ruled out charging others in the case, pending the results of an ongoing review. Army leaders have suggested that there may have been supervisory lapses that allowed the breach to occur.

The release of the State Department cables was denounced by U.S. officials, saying it put countless lives as risk, revealing the identities of people working secretly with the U.S. It also sent shudders through the diplomatic community, as the cables revealed often embarrassing descriptions and assessments of foreign leaders, potentially jeopardizing U.S. relations with its allies.

While thousands of the cables have been released, the bulk of those downloaded have not been made public.

Manning was charged in July with mishandling and leaking classified data and putting national security at risk in connection with the release of a military video of an attack on unarmed men in Iraq.

Army officials said the new charges accuse Manning of using unauthorized software on government computers to extract classified information, illegally download it and transmit the data for public release by what the Army termed "the enemy."

The charges follow seven months of Army investigation.

"The new charges more accurately reflect the broad scope of the crimes that Pvt. 1st Class Manning is accused of committing," said Capt. John Haberland, a legal spokesman for the Military District of Washington.

In a written statement detailing the new charges, the Army said that if Manning were convicted of all charges he would face life in prison, plus reduction in rank to the lowest enlisted pay grade, a dishonorable discharge and loss of all pay and allowances.

Manning's civilian attorney, David Coombs, said any charges that Manning may face at trial will be determined by an Article 32 investigation, the military equivalent of a preliminary hearing or grand jury proceeding, possibly beginning in late May or early June.

Manning's supporters were outraged.

"It's beyond ironic that leaked U.S. State Department cables have contributed to revolution and revolt in dictatorships across the Middle East and North Africa, yet an American may be executed, or at best face life in prison, for being the primary whistleblower," said Jeff Paterson of Courage to Resist, an Oakland, Calif.-based group that is raising funds for Manning's defense.

Trial proceedings against Manning have been on hold since July, pending the results of a medical inquiry into Manning's mental capacity and responsibility.

The 23-year-old Crescent, Okla., native is being held in maximum custody and prevention-of-injury watch at the Marine Corps base in Quantico, Va.

Associated Press writers Lolita C. Baldor in Washington and David Dishneau in Hagerstown, Md., contributed to this report.

http://www.washingtonpost.com/wp-dyn/content/article/2011/03/02/AR2011030205207.html

The NEW YORKER
May 20, 2011

News Desk

Notes on Washington and the world by the staff of *The New Yorker*.

Manning, Assange, and the Espionage Act

by *Raffi Khatchadourian*

The coming week will mark the one-year anniversary of an unusual chapter in the unfolding WikiLeaks saga: the naming of Bradley Manning, a young military-intelligence analyst and Private First Class in the United States Army, as the source of some of the most spectacular classified leaks in this country's history. Manning's role as a WikiLeaks source, reported first at Wired.com, emerged from encrypted online confessions that he apparently made to Adrian Lamo—a former hacker who was secretly recording those confessions, and who later gave them to federal authorities and also made them public. By the time Wired.com published its story, on June 6, 2010, Manning had descended into a labyrinth of military detention, where he has remained (at first, for more than a month without charge). Very few people have been able to talk to him, and his personal defense has not been heard.

Based upon the encrypted confessions, Manning is thought to be the source of all the major WikiLeaks revelations in the past year: the "Collateral Murder" video that I wrote about for *The New Yorker* last summer; the Iraq War Logs and the Afghan War Diary; the State Department cables (which are still being published); and most recently a tranche of files from Camp Delta, at Guantánamo Bay. In contrast, Manning's initial charge sheet, which was finally issued in July, was more modest in its scope. The military accused him of illicitly downloading the "Collateral

Murder" video from a classified network, and giving it to an unauthorized person (presumably from WikiLeaks). It accused him of doing the same with about fifty cables. The only "mass leak" mentioned in the document is one involving "more than 150,000 diplomatic cables," but the military did not accuse Manning of giving them away—just obtaining them unlawfully. This March, however, the military redrafted the charge sheet, and Manning is now formally accused of doing just about everything that he had confessed to doing (and, perhaps, more) in the chat logs.*

In the year that this country has been discussing Bradley Manning, a lot of talk has been devoted to his relationship with Julian Assange, the founder and editor-in-chief of WikiLeaks. This is because the Obama Administration has suggested that it is not content to prosecute Manning alone, but rather is seeking to do so in combination with other potential defendants, specifically Assange, who (the argument goes) may have worked with Manning as an accomplice. This is in no way an easy legal case to make. Manning appears to have broken a very clearly defined set of laws. He may have been driven by recklessness; he may have been driven by morality— by the belief that he was revealing the inner mechanics of unjust policy. But whatever his motivation he seems to have made a rational choice: the public benefit of releasing the material was of greater value to him than the obvious personal legal jeopardy.

As simple as Manning's indictment would appear to be, the legal case against Assange, if there even is one, is murky, with potentially lasting and harmful repercussions to civil liberties in this country. Assange did not obviously break any laws by publishing the leaks that were provided to him. Nevertheless, the Obama Administration has expressed interest in prosecuting him under the Espionage Act, and, if reports about a sitting grand jury convened in Virginia to weigh the matter are true, it may be in the midst of pursuing just such a case. As Jane Mayer noted in *The New Yorker* last week, the act was designed to prevent "classic espionage" and not the release of classified material in a news context. An Espionage Act indictment against Assange would be unprecedented, and could erode freedoms that reporters enjoy during their normal work of cultivating sources in government. I, like other journalists, oppose the idea entirely. The law should not be invoked.

Still, at least publicly, the whole possibility of a case against WikiLeaks has largely come to turn on a single point of fact: did Assange or close associates communicate with Manning? Establishing such a link is a necessary step in trying to prove that there was a conspiracy. Assange has been asked about this, and he has given variations of the same answer. He told George Stephanopoulos on ABC, last year,

I had never heard of the name Bradley Manning before it was published in the press. Wikileaks' technology [was] designed from the very beginning to make sure that we never know the identities or names of people submitting us material. That is, in the end, the only way the sources can be guaranteed that they remain anonymous, as far as we are concerned.

Statements like this may well be true, but they do not address the central question. In the anonymous world of Internet communications, it is possible not to know the name of someone, and still communicate directly with him. Assange himself has used aliases: as a teen-ager, he was known in cyberspace as Mendax.

This January, there were reports that U.S. investigators "could detect no contact between Manning and Assange." That was surprising. Manning's confessions to Lamo make explicit references to direct communications between him and WikiLeaks. At one point, while trying to answer a question, Manning writes, "I'll have to ask Assange." In another burst of short notes, he says:

(2:04:29 PM) im a source, not quite a volunteer
(2:05:38 PM) i mean, im a high profile source… and i've developed a relationship with assange… but i dont know much more than what he tells me, which is very little
(2:05:58 PM) it took me four months to confirm that the person i was communicating was in fact assange

Some people doubt the veracity of these logs. I find this aspect of them to be consistent with what I know and what is reasonable. For a long time now, a compelling bit of corroborating evidence in them has been hidden in plain sight. In May of last year, my piece about WikiLeaks was making its way through the last stages of production at *The New Yorker*. It was being edited and fact-checked; final touches were being added. I did not interview Manning for the article; nonetheless, while we were working on the piece, he wrote to Lamo on May 25th and said, "new yorker is running 10k word article on wl.org on 30 may, btw." This turned out to be a dead-on prediction. But how could he have known specifics about our piece before we had published it? The answer is pretty clear: someone involved in WikiLeaks, or an intermediary, told him.

In the past year, I thought about relaying this little observation in a blog post and have refrained, somewhat out of fear of being subpoenaed or otherwise assisting the Justice Department in a case that I profoundly don't believe in. For a week, I lived in "The Bunker" in Iceland with Assange and Rop Gonggrijp, a Dutch activist who helped in the making of "Collateral Murder," and when their personal records, along with those of Birgitta Jónsdóttir, an Icelandic parliamentarian who was also there, became the target of a federal investigation, I feared that mine would be, too. After all, from my *New Yorker* story it is obvious that I was witness to the making of the "Collateral Murder" video. But I now suspect that I was spared by the same double standard that makes WikiLeaks the subject of a criminal inquiry, and not the New York *Times* or other papers that have published classified material obtained by WikiLeaks (and from elsewhere) in large volumes. I was the *journalist* in the room.

In truth, the argument against an Espionage Act prosecution of Assange should not be built upon a denial that he conversed with Manning—that is, it should not be a fact-dependant argument—but rather should stand on principle. It should *embrace* the notion that they communicated, whether directly, or through an intermediary, or both, because their ability to communicate is exactly what requires protecting. Journalists should be able to talk with sources without fear that they will be "conspirators" to criminality, whether the subject is a NASA shuttle failure or Navy SEALs on a classified raid in Abbottabad. The source typically assumes all of the risk when choosing to reveal information, and must decide if violating the law is worth it. Extending that burden to journalists could have a chilling effect that is larger than any single leak. The Supreme Court appeared to recognize this in its Pentagon Papers ruling. "The responsibility must be where the power is," Justice Potter Stewart wrote. And the power, he observed, clearly resides in government.

Last year, on NPR, Floyd Abrams, who defended the *Times* in the Pentagon Papers case, argued that Assange "has gone a long way down the road of talking himself into a possible violation of the Espionage Act"—implying, as others have, that WikiLeaks is not journalism, and as a result should not be judged by the standards of the First Amendment. Abrams apparently had in mind a line from some very early internal WikiLeaks correspondence that expressed the belief that leaks could "bring down many administrations that rely on concealing reality—including the US administration." Is that really a criminal sentiment? How many Tea Party leaflets express the hope that the Obama Administration will come toppling down? In 2006, when *The Nation* called for the impeachment of President Bush on its cover, should the magazine have been treated as criminally suspect? What if its story had made its case by employing leaked classified intelligence on the killing of civilians in Iraq?

One can find a lot of garbled stuff in Assange's early writings: some of it no more fully formed than thought scribbles, some of it laced with bravado or anger, some of it preoccupied with information warfare rather than the modes of conventional journalism. But in their essence the ideas are shaped around an uncontroversial belief that greater institutional transparency is a good thing, and that technology can advance that aim in radical ways. "Secrecy in government is fundamentally anti-democratic"—that quote isn't from Assange; it's from a concurring opinion that Justice William Douglas wrote in the Pentagon Papers case, but it is a fairly good distillation of the WikiLeaks philosophy. At the same time, there is a difference between an organization's animating principles and how it is managed, and WikiLeaks has not always been run well. Assange is growing much more careful and sophisticated in his editorial decisions, but an observation that Steve Coll made in this magazine last November still holds true today: "If the organization continues to attract sources and vast caches of unfiltered secret documents, it will have to steer through the foggy borderlands between dissent and vandalism, and it will have to defend its investigative journalism against those who perceive it as a crime."

The distinction between the WikiLeaks ideal and its management has become an important, if latent, feature of the debate about Assange. But the First Amendment's protections are not confined to any particular standard of quality in journalism, and not even to journalism as a whole. They extend in various forms to political speech, to religious speech, to poorly articulated speech, and to speech that may interfere with policy, even ongoing military operations. (Did any WikiLeaks revelation have a greater impact on continuing military operations than *Rolling Stone*'s recent profile of General Stanley McChrystal?) Critics of the "Collateral Murder" video—the centerpiece of the original Manning charge sheet— have argued that it is a highly biased production, not an even-handed piece of reporting. So what if it is? The video, a polemic, builds its argument by drawing the viewer's attention to details that Assange believed to be newsworthy in the raw, historical, footage that he had obtained. In that respect, wasn't he acting like an editor, or like any columnist?

It is possible to accept the fact that massive database leaks, such as the Iraq War Logs and the Afghanistan Diaries, present a worrisome development for people in government who require a certain amount of secrecy to function. Technology makes such leaks more readily possible on a scale that is new, and the technology may introduce a qualitative difference in how we must judge such things. But the government is not currently helpless in its ability to prosecute vast database leaks, or to prevent them by non-judicial means—for example, by simply taking better

care of documents. Bradley Manning's detention at Fort Leavenworth is a good example of the power that the military can leverage. Some of Manning's defenders seem to believe that he should not be prosecuted at all, but the government has every right to make its case that he broke the law, and he has every right to defend himself in his upcoming court-martial. Sometime soon, hopefully, we will all get a chance to hear what he has to say.

Read more http://www.newyorker.com/online/blogs/newsdesk/2011/05/manning-assange-and-the-espionage-act.html#ixzz1WXs8uQQU

The New York Times
August 19, 2012

Assange Accuses U.S. of a 'Witch Hunt'
By RAVI SOMAIYA

LONDON — Beyond the reach of police officers waiting to arrest him and with hundreds of supporters looking on, Julian Assange, the founder of WikiLeaks, took to the balcony of Ecuador's embassy here on Sunday to condemn the United States government and cast himself as one of the world's most persecuted whistle-blowers.

Since June, Mr. Assange has been confined to the embassy, a small office in a red-brick apartment block where he fled and was granted asylum from British efforts to extradite him to Sweden. He is wanted for questioning on accusations of rape, sexual molestation and unlawful coercion brought by two women in Stockholm in 2010, allegations he has denied.

On Sunday, with his supporters shouting encouragement, Mr. Assange did not directly mention those allegations or the women who brought them. One supporter who spoke before him, a former British diplomat, Craig Murray, asserted that Mr. Assange had been "fitted up with criminal offenses" as a pretext to prosecute him in the United States for leaking classified government documents.

It was a theme Mr. Assange continued. "I ask President Obama to do the right thing," he said, reading from a statement as he stood on the balcony wearing a crisp blue shirt and red tie, his white hair cut short. "The United States must renounce its witch hunt against WikiLeaks. The United States must dissolve its F.B.I. investigation," a reference to persistent reports that such an investigation is taking place. "The United States must vow that it will not seek to prosecute our staff or our supporters."

A White House spokesman, Josh Earnest, told reporters on Saturday that the Obama administration considered the standoff a matter for the governments of Britain, Sweden and Ecuador.

Mr. Assange's address, which was met with applause and cheers from a crowd that filled the broad streets nearby, was the latest turn in a diplomatic fracas that has captivated London. As he spoke, dozens of Metropolitan Police officers stood by, stony-faced, guarding every entrance and exit of the embassy.

In the embassy, which is legally Ecuadorean territory, Mr. Assange is safe. But should he step foot into the street to begin the journey to a new life in South America, he will be on British territory and subject to arrest.

With neither side willing to back down, and a raid on the embassy deemed unlikely in the face of international law, the diplomatic impasse shows no signs of a quick conclusion.

In granting him asylum on Thursday, President Rafael Correa of Ecuador presented his move as a pre-emptive action against American plans to seek Mr. Assange's extradition and put him on trial in the United States on espionage charges for his role in publishing American military and diplomatic documents. American officials have not publicly disclosed any such plans.

Mr. Assange, 41, an Australian-born hacker who has been both hailed as a champion of free speech and denounced as a danger to public safety, burst onto the scene in 2010 when WikiLeaks posted secret documents on the Iraq war, classified Pentagon documents on the Afghan conflict and hundreds of thousands of classified messages from the United States State Department.

On Sunday, Mr. Assange used his 10-minute speech to criticize the recent prosecutions of those suspected of leaking classified materials.

Specifically, he hailed Pfc. Bradley E. Manning, an Army intelligence analyst accused of passing archives of classified documents to WikiLeaks. He called Private Manning a "hero" and "one of the world's foremost political prisoners." Private Manning faces a court-martial, and a potential life sentence, for what prosecutors have said was his role in transferring the documents to WikiLeaks, which shared them with several news organizations, including The New York Times.

"As WikiLeaks stands under threat," Mr. Assange said, "so does the freedom of expression and the health of all our societies."

He spoke ominously of a "dangerous and oppressive world in which journalists fall silent under the fear of prosecution, and citizens must whisper in the dark."

President Correa has himself been accused of persecuting journalists who have criticized him.

Marc Santora contributed reporting from New York.

http://www.nytimes.com/2012/08/20/world/europe/assange-casts-himself-as-persecuted-whistle-blower.html?_r=1&ref=wikileaks

FRONTLINE:
http://www.pbs.org/wgbh/pages/frontline/foreign-affairs-defense/wikisecrets/court-rulings-set-parameters-of-wikileaks-suspects-trial/

Court Rulings Set Parameters of WikiLeaks Suspect's Trial

January 18, 2013, 6:47 pm ET by Arun Rath

The motive behind the largest intelligence breach in U.S. history will be irrelevant, according to a ruling by Army Judge Col. Denise Lind in a military court in Fort Meade, Md. this week.

This week Judge Lind issued a number of rulings in the case of PFC Bradley Manning, the Army private accused of leaking more than 500,000 documents to WikiLeaks. The judge's ruling on motive was seen as a blow for the defense who will now be prohibited from arguing that Manning may have had a moral reason for leaking the material

Judge Lind also issued a number of other rulings:

- The defense will be allowed to argue that Manning was selective about the kind of information he chose to leak, in order to not damage national security.
- The prosecution will be required to prove that Manning leaked the information knowing that it would fall into the hands of the 'enemy,' namely Al Qaeda. "Aiding the enemy," which could lead to a life sentence, is the most serious charge facing Private Manning.
- The defense will not be allowed to enter into evidence reports from U.S. intelligence services that assess the damage done by the leaks. The judge had earlier ruled that the defense could see the documents, which were discussed in a closed session of the court, but they will not be discussed during the court-martial.

Also this week, the judge heard arguments on the defense team's motion to dismiss all charges because Manning had been denied his right to a speedy trial under the Uniform Code of Military Justice and military court-martial rules. A service member is traditionally entitled to a trial within 120 days of being charged or confined. Manning has been detained for more than 1,000 days since being arrested. The prosecution claims the delays have been justified, given the extraordinary nature of the case, and the need to comb through vast amounts of evidence, but Manning's team is arguing the delay amounts to a violation of Manning's rights.

Judge Lind said she would announce her ruling on the motion to dismiss by Feb. 26. Manning's court-martial is scheduled to begin in June.

The Washington Post
August 21, 2013

Judge sentences Bradley Manning to 35 years
By Julie Tate

A military judge on Wednesday sentenced Pfc. Bradley Manning to 35 years in prison, bringing to a close the government's determined pursuit of the Army intelligence analyst who leaked the largest cache of classified documents in U.S. history.

The long prison term is likely to hearten national security officials who have been rattled by the subsequent leaks from former National Security Agency contractor Edward Snowden. Manning's conviction might also encourage the government to bring charges against the man who was instrumental in the publication of the documents, Julian Assange, the founder of WikiLeaks.

Manning, 25, was acquitted last month of the most serious charge he faced — aiding the enemy — but was convicted of multiple other counts, including violations of the Espionage Act, for copying and disseminating classified military field reports, State Department cables, and assessments of detainees held at Guantanamo Bay, Cuba.

"The message won't be lost for everyone in the military," said Steven Bucci, director of the Douglas and Sarah Allison Center for Foreign Policy Studies at the Heritage Foundation. "When you sign a security clearance and swear oaths, you actually have to abide by that. It is not optional."

Civil liberties groups condemned the judge's decision.

"When a soldier who shared information with the press and public is punished far more harshly than others who tortured prisoners and killed civilians, something is seriously wrong with our justice system," said Ben Wizner, director of the American Civil Liberties Union's Speech, Privacy and Technology Project. "This is a sad day for Bradley Manning, but it's also a sad day for all Americans who depend on brave whistleblowers and a free press for a fully informed public debate."

Manning will receive $3^{1}/_{2}$ years of credit for time served in pretrial confinement and for the abusive treatment he endured in a Marine brig at Quantico, making him eligible for parole in seven years. He will serve his sentence at the military prison at Fort Leavenworth, Kan.

On Wednesday, Manning stood at attention, with his attorneys at his side and his aunt behind him, as he listened to Judge Denise Lind read the sentence aloud. He did not appear to react to her decision.

Lind, an Army colonel, also said Manning would be dishonorably discharged, reduced in rank to private, and forfeit all pay. He had faced up to 90 years in prison.

As Manning was escorted out of the packed courtroom at Fort Meade, more than half a dozen supporters shouted out to him: “We’ll keep fighting for you, Bradley! You’re our hero!”

According to his attorney David Coombs, Manning told his distraught defense team after the sentence was issued, “It’s okay. Don’t worry about it. I know you did your best. I am going to be okay. I am going to get through this.”

Coombs said at a news conference that he will seek a presidential pardon for his client in the coming weeks. He read a statement from Manning in which the private reiterated his reasons for leaking classified material, saying he had “started to question the morality” of U.S. policy. Manning added that if his request for a pardon is denied, he will serve his time “knowing sometimes you pay a heavy price to live in a free country.”

“I will gladly pay that price if it means we could have a country that is truly conceived in liberty and dedicated to the proposition that all women and men are created equal,” he said.

White House spokesman Josh Earnest said any application will receive routine consideration. The administration had no further comment on the sentence, and military prosecutors also did not comment on the sentence.

In a statement, WikiLeaks called Manning’s conviction “an affront to basic concepts of Western justice” and said his treatment has been intended “to send a signal to people of conscience in the U.S. government who might seek to bring wrongdoing to light.”

Coombs said recent disclosures about NSA surveillance had eclipsed the attention paid to Manning’s court-martial. Asked how he would advise Snowden on the possibility of returning to the United States for trial, Coombs said: “I would tell him the current environment is not one friendly to whistleblowers.”

“Under the current administration, leaking information to the press is tantamount to aiding the enemy. We avoided a conviction on the aiding the enemy charge, but the fact that they pursued it, let it go forward, should send alarms to all journalists,” he added.

Coombs said the prosecution had offered Manning a plea deal before trial in order to get him to testify against WikiLeaks in an ongoing investigation in the Eastern District of Virginia. Coombs said the government offer was “a length of sentence that exceeded what Manning received today,” and was rejected.

“I do not think the sentence has a legal effect on the continued investigation of Julian Assange and WikiLeaks,” said Michael Ratner, the U.S. attorney for Assange and WikiLeaks and president emeritus of the Center for Constitutional Rights. “However, it may well embolden the government in its efforts to indict journalists such as Julian Assange. The length of the sentence demonstrates what Assange and Edward Snowden face if they are ever taken into custody by the U.S. — draconian sentences.”

The court-martial will now enter a "post-trial" and appellate phase. The government is required to compile a complete record, review all transcripts and findings, and submit its final version to a military official known as the convening authority, Maj. Gen. Jeffrey S. Buchanan. Manning can petition Buchanan for clemency during this phase. Manning's case will also be reviewed by the Army Court of Criminal Appeals, which will decide whether the verdict and sentence can be appealed.

Manning established a relationship online with a person who is thought to be Assange in 2010.

He transmitted the first documents to WikiLeaks in February 2010, sending what came to be known as the Iraq and Afghanistan "War Logs." He continued to transmit more material, including a video that showed a U.S. Apache helicopter in Baghdad opening fire on a group of individuals that the crew believed to be insurgents. Among the dead were Iraqi children and two journalists.

Manning was arrested in Iraq in May 2010.

http://www.washingtonpost.com/world/national-security/judge-to-sentence-bradley-manning-today/2013/08/20/85bee184-09d0-11e3-b87c-476db8ac34cd_story.html